Организация Объединенных Наций ECE/TRANS/WP.29/2021/59

Экономический и Социальный Совет

Distr.: General
22 December 2020
Russian
Original: English

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Всемирный форум для согласования правил в области транспортных средств

Сто восемьдесят третья сессия
Женева, 9–11 марта 2021 года
Пункт 4.2.3 предварительной повестки дня
Указания, запрошенные рабочими группами по вопросам, связанным с правилами ООН, прилагаемыми к Соглашению 1958 года: Толкование отдельных правил ООН

Предложения по документам о толковании Правил № 155 ООН (кибербезопасность и система управления кибербезопасностью)

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

Воспроизведенный ниже текст был подготовлен Рабочей группой по автоматизированным/автономным и подключенным транспортным средствам (GRVA) на ее сессии в сентябре 2020 года. Он был одобрен Всемирным форумом для согласования правил в области транспортных средств (WP.29) на его сессии в ноябре 2020 года на основе неофициального документа (WP.29-182-05). WP.29 поручил секретариату распространить этот документ под официальным условным обозначением на сессиях, которые состоятся в марте 2021 года (ECE/TRANS/WP.29/1155, п. 77).

* В соответствии с программой работы Комитета по внутреннему транспорту на 2020 год, изложенной в предлагаемом бюджете по программам на 2020 год (A/74/6 (часть V, разд. 20), п. 20.37), Всемирный форум будет разрабатывать, согласовывать и обновлять правила ООН в целях повышения эффективности транспортных средств. Настоящий документ представлен в соответствии с этим мандатом.

** Настоящий документ был запланирован к изданию после установленного срока в силу обстоятельств, не зависящих от представившей его стороны.

A. Часть A

1. Преамбула

1.1 Цель части A настоящего документа — оказать содействие в разъяснении требований пунктов 5, 7 и 8 приложения 1 к Правилам ООН о единообразных предписаниях, касающихся официального утверждения транспортных средств в отношении кибербезопасности и системы управления кибербезопасностью (Правила № 155 ООН), и представить информацию о том, что можно использовать в целях обоснования этих требований. Целевая аудитория в контексте данного документа включает изготовителей транспортных средств, представляющих соответствующие системы в целях проведения испытаний, и технические службы/органы по официальному утверждению, которые производят оценку этих систем. В конечном итоге настоящий документ должен содействовать согласованию испытаний в рамках различных технических служб/органов по официальному утверждению.

2. Примечание, касающееся обоснования требований

2.1 Настоящий документ является лишь руководством. В нем содержится информация о том, какие именно данные могут быть/будут приемлемы для технических служб/органов по официальному утверждению и какой именно уровень данных может быть обеспечен. Он не призван быть исчерпывающим. Стандарты, на которые делаются ссылки, приводятся в качестве примеров и не носят обязательный характер. Тем не менее проверка согласованности (см. раздел 6 «Ссылка на ISO/SAE DIS 21434 (E)») показала, что именно ISO/SAE DIS 21434 может оказать существенную поддержку во внедрении практику требований к СОКиБ тем организациям, которые входят в состав производственно-сбытовых цепочек. Следует иметь в виду, что положения ISO/SAE DIS 21434, на которые делается ссылка, могут измениться на более поздней редакции этого стандарта, однако, как ожидается, этот стандарт будет по-прежнему соответствовать этим требованиям. В зависимости от типа транспортного средства, определенного изготовителем транспортного средства, а также практики и процедур, используемых ими, могут предоставляться альтернативные и/или равноценные данные.

2.2 Что касается всех требований Правил, то их соответствие может быть доказано с помощью соответствующей документации/презентации и/или аудиторской проверки. Формат, в котором представляется документация, носит открытый характер, однако он подлежит согласованию на уровне изготовителей транспортных средств и технических служб/органов по официальному утверждению до проведения испытаний/аудиторской проверки. Соответствующее подтверждение можно сделать в виде обзора, диаграмм и опытным путем. Аргумент в пользу того, что требования выполняются, должен быть логичным, понятным и убедительным. Документы не обязательно должны быть большими.

2.3 Формулировки, используемые в настоящем документе, направлены на соблюдение Директив ИСО/МЭК, часть 2 «Принципы и правила построения и разработки документов ИСО и МЭК» (ISBN 978-92-67-10603-8), описанных в разделе 7 восьмого издания 2018 года.

3. Руководство по требованиям к Правилам о единообразных предписаниях, касающихся официального утверждения транспортных средств в отношении кибербезопасности и системы управления кибербезопасностью (Правила № 155 ООН)

Примечание. Пункты, упомянутые ниже, относятся к пунктам единообразных предписаний, касающихся официального утверждения транспортных средств в отношении кибербезопасности и системы управления кибербезопасностью.

A. Пункты 1–4 Правил

«1. Область применения»

Никаких руководящих указаний в отношении этого требования в настоящий документ внесено не было.

«2. Определения»

Никаких руководящих указаний в отношении этого требования в настоящий документ внесено не было.

«3. Заявка на официальное утверждение»

Никаких руководящих указаний в отношении этого требования в настоящий документ внесено не было.

«4. Маркировка»

Никаких руководящих указаний в отношении этого требования в настоящий документ внесено не было.

B. Пункты 5–5.3

«5. Официальное утверждение»

«5.3 Органы по официальному утверждению не предоставляют никакого официального утверждения типа, не убедившись в том, что изготовитель ввел в действие удовлетворительные механизмы и процедуры, позволяющие надлежащим образом регулировать аспекты кибербезопасности, охватываемые настоящими Правилами».

Разъяснение требования

В дополнение к условиям, указанным в пункте 5.1, орган по официальному утверждению обязан проверить, были ли должным образом выполнены все требования, указанные в разделе 7 Правил. К ним относится система управления кибербезопасностью, упомянутая в пунктах 7.2 и 7.3.1.

C. Пункт 5.3.1, часть a)

«5.3.1 Орган по официальному утверждению и его технические службы обеспечивают, помимо критериев, изложенных в приложении 2 к Соглашению 1958 года:

a) наличие у них компетентного персонала, обладающего соответствующими навыками в области кибербезопасности и конкретными знаниями рисков причинения вреда в области автомобилестроения;».

Разъяснение требования

Это требование будет означать, что орган или техническая служба (организация) имеет в своем распоряжении достаточное количество сотрудников следующих категорий:

a) сотрудники, обладающие компетенцией и опытом в деле применения правил по кибербезопасности, а также любых национальных или ведомственных правил, стандартов и процедур, необходимых для их выполнения и применения. Применимые стандарты могут включать ISO 21434 и ISO 27001 в части содержания и соответствующих аспектов ISO 19011 и ISO PAS 5112 в части процессов аудиторской проверки;

b) сотрудники, обладающие компетенцией и опытом в деле применения методов лабораторной проверки кибербезопасности, таких как перьевое тестирование, случайное тестирование и тестирование боковых каналов, применительно к кибербезопасности транспортного средства.

Такая компетенция должна быть подтверждена соответствующим аттестатом или другими равноценными документами, удостоверяющими факт профессиональной подготовки.

Настоящие Правила не устанавливают каких бы то ни было конкретных договорных отношений между органом по официальному утверждению/технической службой и соответствующими сотрудниками. Это может быть трудовое соглашение (договор найма), контракт на оказание услуг и т. д.

Штат соответствующих сотрудников должен быть пропорционален фактической рабочей нагрузке.

Внутренние процедуры организации должны обеспечивать выполнение или эффективный контроль за выполнением задач на основании Правил сотрудниками, которые обладают соответствующими навыками.

D. Пункт 5.3.1, часть b)

«b) выполнение ими процедур единообразной оценки в соответствии с настоящими Правилами;»

Разъяснение данного требования

Организация должна иметь процедуры, обеспечивающие проведение оценки каждого типа транспортного средства по одной и той же схеме. При необходимости эта оценка может включать соответствующие варианты. Применение вариантов определяется четкими критериями, которые должны быть изложены и разъяснены во внутренней документации организации.

В том случае если орган по официальному утверждению назначил несколько технических служб, он должен обеспечить единообразие оценки между различными техническими службами, в частности путем организации регулярных встреч, на которых происходит обмен опытом.

В организации должны быть налажены процессы безопасного хранения и передачи конфиденциальной информации.

Технические службы должны наладить процессы, обеспечивающие добросовестное отношение сотрудников, которые занимаются оценкой с учетом соответствующих рисков.

Это требование Правил не может считаться выполненным путем простого установления требуемых процессов и процедур. Оно предполагает также их эффективное применение, что в свою очередь подразумевает необходимость соответствующей подготовки и эффективного контроля качества.

Примеры документов/доказательственных данных, подтверждающих правильность реализации

Пояснительные документы технических служб

Руководящие принципы передовой практики органа по официальному утверждению. Настоящие положения являются сводными вариантами пояснительных документов технических служб.

Протоколы совещаний органа по официальному утверждению типа и технических служб, касающиеся обмена опытом.

E. Пункт 5.3.2

«5.3.2 Каждая Договаривающаяся сторона, применяющая настоящие Правила, уведомляет и информирует по линии своего органа по официальному утверждению другие органы по официальному утверждению о методе и критериях, взятых за основу уведомляющим органом в порядке оценки уместности мер, принятых в соответствии с настоящими Правилами, в частности с пунктами 5.1, 7.2 и 7.3.

Эта информация доводится до сведения только перед первым предоставлением официального утверждения на основании настоящих Правил и каждый раз при обновлении метода или критериев оценки.

Эта информация предназначена для общего пользования в целях сбора и анализа передовой практики и обеспечения единообразного применения настоящих Правил всеми органами по официальному утверждению, применяющими настоящие Правила».

Разъяснение требования

Это требование имеет целью обеспечить согласование порядка применения требований пунктов 5.1, 7.2 и 7.3 на уровне Договаривающихся сторон. Важно иметь в виду, что нижеследующие подпункты следует толковать таким образом, чтобы это позволило достичь поставленной цели. Кроме того, обмен данными должен позволить взаимно изучать и накапливать передовой опыт, который может послужить источником вдохновения для дальнейшей работы по внесению поправок в Правила № [155] ООН в будущем.

Как можно судить в результате сопоставления формулировок пунктов 5.3.2 и 5.3.3, информация о методах и критериях должна содержать:

a) минимальные уровни эффективности, которые должны обеспечиваться по требованию органа по официальному утверждению в части спецификаций, предусмотренных в пунктах 7.2 и 7.3;

b) меры и процессы, которым должны следовать органы по официальному утверждению/их технические службы в ходе оценки соответствия после подачи заявки на официальное утверждение типа.

В частности, эта информация должна включать:

c) характеристики и минимальные критерии эффективности, которым должны удовлетворять процессы, упомянутые в пункте 7.2.2.2, в том числе информацию о критериях, используемых для подтверждения того, что риски, упомянутые в пункте 7.2.2.2. d), «устраняются надлежащим образом»;

d) критерии, которые будет применять орган по официальному утверждению для оценки того, обеспечивают ли эти процессы снижение в разумные сроки уровня киберугроз и факторов уязвимости, упомянутых в пункте 7.2.2.3, включая информацию об условиях, в которых уровень этих угроз и факторов уязвимости будет считаться сниженным, и о том, что понимается под «разумными сроками»;

e) критерии, которые будет применять орган по официальному утверждению для оценки соответствия этих процессов требованию, указанному в пункте 7.2.2.4;

f) критерии, которые будет применять орган по официальному утверждению для оценки того, подтвердил ли изготовитель тот факт, что СОКиБ регулирует факторы зависимости, упомянутые в пункте 7.2.2.5;

g) критерии, которые будет применять орган по официальному утверждению для оценки того, будет ли считаться свидетельство СОКиБ приемлемым в случае данного типа транспортного средства, подлежащего официальному утверждению;

h) в случае официального утверждения типа транспортного средства до 1 июля 2024 года критерии, которые будет применять орган по официальному утверждению для оценки того, был ли учтен фактор кибербезопасности на этапе разработки данного типа транспортного средства таким образом, чтобы был обеспечен эквивалентный показатель кибербезопасности;

i) критерии, которые будет применять орган по официальному утверждению для оценки того, принял ли изготовитель достаточные меры в целях выявления и регулирования рисков, связанных с поставщиками, в случае данного типа транспортного средства, подлежащего официальному утверждению, включая требуемые нормы регулирования таких рисков;

j) критерии, которые будет применять орган по официальному утверждению для оценки того, выявил ли изготовитель транспортного средства критические элементы типа транспортного средства, включая определение «критических элементов», которое было принято данным органом в этих целях;

k) критерии, которые будет применять орган по официальному утверждению для оценки того, провел ли изготовитель транспортного средства исчерпывающую оценку риска для данного типа транспортного средства, как это требуется в соответствии с подпунктом 7.3.3 настоящих Правил;

l) критерии, которые будет применять орган по официальному утверждению для оценки того, обеспечивается ли защита данного типа транспортного средства от рисков, выявленных в ходе оценки риска изготовителем транспортного средства;

n) критерии, которые будет применять орган по официальному утверждению для оценки того, являются ли меры по снижению воздействия, применяемые изготовителем, соразмерными, включая разъяснение термина «соразмерные»;

o) критерии, которые будет применять орган по официальному утверждению для оценки того, являются ли меры по снижению воздействия, указанные в части B или C приложения 5, неактуальными, недостаточными для выявленного риска или неосуществимыми;

p) критерии, которые будет применять орган по официальному утверждению для оценки того, будет ли «надлежащей» в соответствии с подпунктом 7.3.4 «иная мера по снижению воздействия»;

q) критерии, которые будет применять орган по официальному утверждению для оценки того, были ли испытания, проведенные изготовителем для проверки эффективности принятых мер безопасности, «надлежащими» и «достаточными»;

r) критерии, которые будет применять орган по официальному утверждению для оценки того, являются ли меры, принимаемые изготовителем в целях обеспечения особых условий на данном типе транспортного средства для хранения и использования послепродажного программного обеспечения, услуг, приложений или данных, «надлежащими» и «соразмерными», в том числе разъяснение толкования термина «соразмерные» в этом контексте;

s) документы, которые потребуются органу по официальному утверждению, для проверки того, принял ли изготовитель транспортного средства необходимые меры, упомянутые в подпункте 5.1.1;

t) проверки, которые будет проводить орган по официальному утверждению или техническая служба, и стратегия проверки, которую они будут применять с целью убедиться в том, что изготовитель данного транспортного средства принял надлежащие меры по обеспечению кибербезопасности и оформил их документально;

u) внутренние процедуры, которые будет применять орган по официальному утверждению в процессе оценки в соответствии с разделом 5 Правил.

Важно подчеркнуть тот факт, что органы Сторон по официальному утверждению косвенно обязаны следовать методам и требованиям, которые подлежат совместному использованию и оценке.

F. Пункт 5.3.3

«5.3.3 Информация, указанная в пункте 5.3.2, загружается на английском языке в защищенную базу данных в Интернете (ДЕТА), созданную Европейской экономической комиссией Организации Объединенных Наций, в установленные сроки и не позднее чем за 14 дней до первого предоставления официального утверждения на основании соответствующих методов и критериев оценки. Эта информация должна быть достаточной для понимания минимальных уровней эффективности, которые были приняты органом по официальному утверждению в отношении каждого конкретного требования, указанного в пункте 5.3.2, а также процессов и мер, которые он применяет для проверки соблюдения этих минимальных уровней эффективности».

Разъяснение требования

Загружаемая информация должна быть объективно достаточной для понимания минимальных уровней эффективности, принятых соответствующим органом, по мнению которого требования Правил соблюдаются. Этот момент имеет важнейшее значение с учетом высокого уровня и частого использования общих положений в процессе разработки таких требований.

Хотя обязательство обмениваться информацией, о котором говорится в пункте 5.3.3, представляет собой обязательство результата, которое всегда должно выполняться органом по официальному утверждению, тем не менее он должен выполнять это обязательство, исходя из необходимости не допустить создания угрозы для кибербезопасности транспортного средства, тип которого был официально утвержден на основании настоящих Правил.

Предпочтительно сделать так, чтобы информация предоставлялась другим органам заблаговременно (т. е. задолго до проведения первой оценки в соответствии с этими методами и критериями), с тем чтобы другие органы могли изучить ее и при необходимости получить дополнительные разъяснения, что позволило бы полностью достичь поставленных целей. Вместе с тем орган по официальному утверждению не может ни при каких обстоятельствах предоставить официальное утверждение типа на основе таких методов и критериев менее чем за 14 дней с момента обмена информацией через базу данных ДЕТА.

Примеры документов/доказательственных данных, которые могут быть предоставлены

См. приложение 1, в котором представлена типовая форма обмена данными по линии ДЕТА в соответствии с пунктом 5.3.

G. Пункт 5.3.4

«5.3.4 Органы по официальному утверждению, получающие информацию, указанную в пункте 5.3.2, могут направить свои замечания уведомляющему органу по официальному утверждению путем их загрузки в ДЕТА в течение 14 дней со дня уведомления».

Разъяснение требования

Органам по официальному утверждению других Договаривающихся сторон предоставляется возможность изложить замечания в отношении направленной им информации, но делать это они не обязаны.

Этот 14-дневный срок применяется также в том случае, если информация, указанная в соответствии с пунктом 5.3.2, была представлена ранее, чем за 14 дней до принятия решения об официальном утверждении. В идеальном случае замечания других органов следует обсудить и, если они являются правомерными/полезными, принять во внимание до того, как будут применены в первый раз методы и критерии, используемые по линии ДЕТА на совместной основе. Поэтому заинтересованные органы по официальному утверждению должны реагировать как можно быстрее, направляя свое мнение в данный орган по официальному утверждению.

H. Пункт 5.3.5

«5.3.5 Если орган по официальному утверждению не в состоянии принять во внимание замечания, полученные в соответствии с пунктом 5.3.4, то органы по официальному утверждению, направившие замечания, и орган, предоставляющий официальное утверждение, обращаются за дополнительными разъяснениями в соответствии с приложением 6 к Соглашению 1958 года. Соответствующая вспомогательная Рабочая группа Всемирного форума для согласования правил в области транспортных средств (WP.29), занимающаяся настоящими Правилами, согласовывает общее толкование методов и критериев оценки. Это общее толкование подлежит применению, и в этом случае все органы по официальному утверждению предоставляют официальные утверждения типа на основании настоящих Правил».

Разъяснение требования

Возможные замечания органов по официальному утверждению других Договаривающихся сторон не имеют приостанавливающего действия в отношении выдачи официального утверждения типа органом, предоставляющим данное официальное утверждение. Вместе с тем если этот орган решит не принимать эти замечания к сведению, то органы, высказавшие замечания, и орган по официальному утверждению, который принял такое решение, обязаны инициировать обсуждение представленных методов и критериев, а также полученных замечаний на уровне GRVA. Хотя обязанность запрашивать дальнейшие разъяснения возлагается на оба органа, тем не менее начинать процедуру в соответствии с приложением 6, с тем чтобы орган, представивший информацию, и орган, высказавший замечания, предприняли официальные шаги в этом направлении, необходимости нет. В соответствии с пунктом 3 приложения 6 «определять вопросы, возникающие в связи с разногласиями в толковании» Правил по кибербезопасности, должен Председатель GRVA.

В вопросах толкования GRVA должна ставить во главу угла цель процедуры консультаций, указанной в пункте 5.3.2, обеспечивая тем самым сближение позиций в вопросах применения данных Правил. Поэтому они должны содержать элементы, позволяющие четко установить, являются ли минимальные уровни эффективности и процедуры, применяемые органом по официальному утверждению, достаточными/надлежащими для проверки соблюдения требований этих Правил. После того как GRVA согласится с этим толкованием данных Правил, оно должно применяться всеми органами по официальному утверждению во всех будущих процедурах оценки (применительно к официальным утверждениям типа, изменениям и распространению)

в соответствии с данными Правилами. Это может обусловить необходимость обновления существующих методов и критериев компетентными органами некоторых или всех Договаривающихся сторон.

I. Пункт 5.3.6

«5.3.6 Каждый орган по официальному утверждению, предоставляющий официальное утверждение типа на основании настоящих Правил, уведомляет другие органы по официальному утверждению о предоставленном официальном утверждении. Официальное утверждение типа вместе с дополнительной документацией загружается на английском языке в ДЕТА органом по официальному утверждению в течение 14 дней после дня предоставления официального утверждения».

Разъяснение требования

Это требование отличается от требования об уведомлении на основе стандартной формы, предусмотренного в пункте 5.2, и дополняет его. Уведомление об официальном утверждении следует направлять вместе с дополнительной документацией, которая не указана в пункте 5.3.6. Цель обмена информацией в Правилах не указана, но на основании пункта 5.3.7 можно сделать вывод о том, что ее смысл сводится к тому, чтобы позволить органам по официальному утверждению «изучать» эти официальные утверждения и, возможно, учитывать «различные мнения» в соответствии, в частности, с приложением 6. Поэтому дополнительная документация должна включать все элементы (в том числе протоколы испытаний), достаточные для того, чтобы дать органам по официальному утверждению возможность понять, применялись ли методы и критерии, упомянутые в предыдущих пунктах, в контексте соответствующего индивидуального решения по поводу того или иного официального утверждения, и если да, то каким образом.

Эта информация должна быть загружена в базу данных ДЕТА. Типовая форма загрузки информации в базу данных приведена в разделе 5.

Обязательство относительно уведомления, указанного в первом предложении пункта 5.3.6, не ставится в зависимость от возможности согласования требования, предусматривающего загрузку этой информации в ДЕТА, с обязательствами по национальному законодательству, регламентирующими вопросы безопасности и возможной конфиденциальности передаваемой информации. В том случае если загрузка информации в ДЕТА может противоречить таким другим обязательствам, то орган по официальному утверждению должен найти способ уведомить об этом безопасным способом.

J. Пункт 5.3.7

«5.3.7 Договаривающиеся стороны могут изучать выданные официальные утверждения на основе информации, загруженной в соответствии с пунктом 5.3.6. В случае каких-либо разногласий в толковании между Договаривающимися сторонами этот момент должен быть урегулирован в соответствии со статьей 10 и приложением 6 к Соглашению 1958 года. Договаривающиеся стороны информируют также соответствующую вспомогательную рабочую группу Всемирного форума для согласования правил в области транспортных средств (WP.29) о разногласиях в толковании по смыслу приложения 6 к Соглашению 1958 года. Соответствующая Рабочая группа содействует урегулированию проблемы разногласий в толковании и в случае необходимости может проконсультироваться по этому вопросу с WP.29».

Разъяснение требования

В случае «разногласий в толковании» по поводу информации, касающейся официального утверждения типа, между органами по официальному утверждению, делается ссылка на статью 10 Соглашения и приложение 6. Процедура, предусмотренная статьей 10, зарезервирована на тот случай, когда по поводу

толкования Соглашения возникают разногласия. И напротив, любые споры, возникающие в контексте официального утверждения типа и касающиеся применения или толкования Правил (а следовательно, и применения методов и критериев, упомянутых в пункте 5.3.3), должны разрешаться в соответствии с пунктом 2 приложения 6.

K. Пункты 6–7.1.1

«6. Свидетельство о соответствии системы обеспечения кибербезопасности»

Никаких руководящих указаний в отношении этого требования в настоящий документ внесено не было.

«7. Технические требования

7.1 Общие технические требования

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

Разъяснение требования

Требования настоящих Правил не должны ограничивать положения или требования других правил ООН, а также национального или регионального законодательства, описанных в пунктах 1.3 и 1.4 области применения настоящих Правил.

L. Пункты 7.2–7.2.1

«7.2 Требования, предъявляемые к системе обеспечения кибербезопасности

7.2.1 В целях оценки орган по официальному утверждению или его техническая служба удостоверяется в том, что у изготовителя транспортного средства есть соответствующая система обеспечения кибербезопасности, и удостоверяется в ее соответствии настоящим Правилам».

Разъяснение требования

Это требование имеет целью обязать техническую службу или орган по официальному утверждению, удостоверится в том, что:

a) у изготовителя транспортного средства есть СОКиБ;

b) представленная СОКиБ соответствует требованиям, перечисленным ниже в настоящих Правилах.

В случае этого требования основное внимание должно уделяться производственным процессам и оценке их наличия с целью получить представление о способности изготовителя соблюдать требования СОКиБ.

В этой связи необходимо принять к сведению следующие уточнения:

c) СОКиБ может быть частью системы управления качеством работы данной организации или быть независимой от нее;

d) если СОКиБ является частью СРК организации, то она должна быть четко идентифицируемой.

Примеры документов/доказательственных данных, которые могут быть предоставлены

Могут применяться следующие стандарты:

e) в качестве основы для подтверждения и оценки СОКиБ можно использовать ISO/SAE 21434. Для оценки СОКиБ в целом можно использовать позиции 5 «Общее управление системой кибербезопасности», 6 «Управление системой кибербезопасности в зависимости от проектов» и 7 «Непрерывная деятельность в области кибербезопасности»;

f) к соответствующим частям СОКиБ могут применяться стандарты ISO 18045, ISO 15408, стандарты серии ISO 27000 и стандарты серии ISO 31000.

M. Пункты 7.2.2–7.2.2.1

«7.2.2 Система обеспечения кибербезопасности охватывает следующие аспекты:

7.2.2.1 Изготовитель транспортного средства подтверждает органу по официальному утверждению или его технической службе, что их система обеспечения кибербезопасности применяется к следующим этапам:

- этап разработки;
- этап реализации;
- этап после реализации».

Разъяснение требования

Цель этого требования — обеспечить такое положение, при котором система управления кибербезопасностью должна быть в состоянии показать, каким образом изготовитель будет обеспечивать кибербезопасность в течение срока эксплуатации транспортных средств, изготовленных в соответствии с тем или иным типом транспортного средства. Это включает в себя подтверждение наличия процедур и процессов, охватывающих три этапа. На каждом из этапов жизненного цикла могут выполняться конкретные действия.

Пункт 7.2.2.1 описывает различные этапы жизненного цикла данного типа транспортного средства, подлежащие рассмотрению в рамках СОКиБ, а пункт 7.2.2.2 применяется ко всем этим этапам, если не указано иное. Эти этапы также применимы к пункту 7.2.2.4.

СОКиБ может включать активные и/или реактивные процессы или процедуры, включая завершение этапа эксплуатационной поддержки того или иного типа транспортного средства, а также способ их реализации или приведения в действие. Это может включать возможность отключения необязательных функций/систем и условия, при которых это может произойти.

Эксплуатационный срок службы (этап использования) того или иного транспортного средства начинается на этапе производства данного типа транспортного средства. Он заканчивается либо на этапе производства, либо на этапе после производства данного типа транспортного средства.

Примеры документов/доказательственных данных, которые могут быть предоставлены

Могут применяться следующие стандарты:

a) в качестве основы для подтверждения и оценки требуемых этапов СОКиБ можно воспользоваться стандартом ISO/SAE 21434. Для оценки этапа разработки СОКиБ можно использовать позиции 9 «Этап разработки концепции», 10 «Разработка продукта» и 11 «Валидация кибербезопасности». Для оценки производственного этапа СОКиБ можно использовать позицию 12 «Производство». Для оценки этапа после производства СОКиБ можно использовать позиции 7 «Непрерывная деятельность по обеспечению кибербезопасности», 13 «Эксплуатация и техническое обслуживание» и 14 «Вывод из эксплуатации»;

b) другие стандарты, которые можно применить к пункту 7.2.2, и его отдельным требованиям, включают: ISO 18045, ISO 15408, стандарты серии ISO 27000 и стандарты серии ISO 31000.

N. Пункт 7.2.2.2, часть a)

«7.2.2.2 Изготовитель транспортного средства подтверждает, что процессы, используемые в рамках его системы обеспечения кибербезопасности, позволяют надлежащим образом учитывать вопросы безопасности, включая риски и меры по смягчению последствий, перечисленные в приложении 5. Это включает следующее:

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

Разъяснение требования

Цель этого требования — обеспечить наличие в организации соответствующих процессов введения в действие СОКиБ. Сфера охвата этого требования ограничивается процессами, которые имеют отношение к кибербезопасности данных типов транспортных средств, а не к другим аспектам работы организации. Например, сфера действия этого требования, как предполагается, не будет распространяться на всю систему управления информационной безопасностью той или иной организации.

Для того чтобы показать тот спектр деятельности, которую осуществляет изготовитель для управления кибербезопасностью на этапах разработки, производства и послепродажного обслуживания транспортного средства того или иного типа, можно было бы использовать следующие аспекты:

a) организационную структуру, используемую для решения вопросов кибербезопасности;

b) роли и обязанности, касающиеся управления кибербезопасностью, включая подотчетность.

Примеры документов/доказательственных данных, которые можно было бы представить

c) в качестве основы для подтверждения и оценки работы можно воспользоваться в случае необходимости стандартом ISO/SAE 21434, в особенности на основе [RQ-05-01], [RQ-05-02], [RQ-05-07], [RQ-05-08];

d) для подтверждения этого требования можно воспользоваться спецификацией BSI PAS 1885. Для подтверждения организационных процессов соответствующего изготовителя можно воспользоваться национальными схемами сертификации, такими как «UK Cyber Essentials».

Данное требование следует считать невыполненным, если справедливо одно из следующих утверждений

1. Процессы отсутствуют или не завершены.

2. Процессы не применяются на всесторонней или последовательной основе.

3. Процессы зачастую или регулярно идут в обход установленных требований для достижения бизнес-целей.

4. Подход изготовителя транспортных средств к системе управления безопасностью и рисками не имеет никакого отношения к его процессам.

5. Безопасность системы полностью зависит от тщательного и последовательного применения пользователями ручных процессов обеспечения безопасности.

6. Процессы не пересматривались ни в порядке реагирования на серьезные изменения (например, в области технологии или нормативной базы), ни в течение подходящего периода времени.

7. Процессы труднодоступны для персонала, слишком детализированы, чтобы их можно было запомнить, или слишком сложны для понимания.

Данное требование можно считать выполненным, если справедливы все следующие утверждения

1. Изготовитель транспортных средств полностью оформляет документально свой общий подход к управлению безопасностью и рисками, практику в области техники безопасности и порядок соблюдения конкретных норм. Система кибербезопасности интегрирована и встроена во все эти процессы, а ключевые показатели эффективности доводятся до сведения соответствующих руководящих органов.

2. Заводские процессы изготовления транспортных средств разрабатываются таким образом, чтобы они были практичными, удобными и соответствовали принятым стратегиям и технологиям.

3. Процессы, в основу которых положены поведенческие навыки пользователя, носят практичный, адекватный и достижимый характер.

4. Изготовитель транспортного средства регулярно проверяет и обновляет процессы с целью обеспечить их актуальность. Это следует делать в дополнение к обзорам после какого-либо крупного инцидента в сфере кибербезопасности.

5. Любые изменения, которые вносятся в основную функцию, или угроза, которой она подвергается, автоматически влекут за собой пересмотр действующих процессов.

6. Системы изготовителей транспортных средств строятся таким образом, чтобы они были и оставались безопасными даже в том случае, когда пользователь не всегда соблюдает стратегии и процессы в области безопасности. Такое утверждение предполагает необходимость соответствующего обоснования.

O. Пункт 7.2.2.2, часть b)

«b) процессы, используемые для выявления рисков, которым подвергаются транспортные средства. В рамках этих процессов будут рассмотрены угрозы, указанные в части A приложения 5, а также другие соответствующие угрозы;»

Разъяснение требования

Цель этого требования заключается в следующем: изготовитель должен продемонстрировать процессы и процедуры, которые он использует для выявления рисков, которым подвергаются соответствующие типы транспортных средств.

Используемые процессы должны строиться с учетом всех вероятных источников риска. К ним относятся риски, указанные в приложении 5 к Правилам по кибербезопасности, например риски, связанные с подключенными услугами или факторами зависимости, которые являются внешними по отношению к транспортному средству.

Источники, подлежащие идентификации риска, могут указываться. Они могут включать:

a) платформы обмена информацией о факторах уязвимости/угрозах;

b) уроки, извлеченные в связи с соответствующими рисками и факторами уязвимости.

Примеры документов/доказательственных данных, которые могут быть предоставлены

В этой связи могут применяться следующие стандарты:

c) ISO/SAE 21434, в особенности на основе [RQ-08-01], [RQ-08-02], [RQ-08-08], [RQ-08-09].

В ходе используемых процессов могут быть рассмотрены следующие моменты:

d) определение значимости системы в плане кибербезопасности;

e) описание всей системы в целом с точки зрения:

i) определения системы/функции;

ii) граничных условий и взаимодействия с другими системами;

iii) архитектуры;

iv) условий эксплуатации системы (контекст, ограничения и допущения);

f) идентификация ресурсов;

g) идентификация угроз;

h) идентификация факторов уязвимости.

Данное требование следует считать невыполненным, если справедливо одно из следующих утверждений

1. Идентификация риска не строится на четко определенном наборе допущений.

2. Идентификация риска для типов транспортных средств является «разовым» мероприятием (или не производится вообще).

3. Типы транспортных средств оцениваются на индивидуальной основе, без учета факторов зависимости от других систем и взаимодействия с ними (например, взаимодействие между ИТ- и ОТ-средами).

Данное требование можно считать выполненным, если справедливы все следующие утверждения

1. Организационный процесс изготовителя транспортных средств обеспечивает выявление, анализ, определение приоритетности и управление рисками в области безопасности для данных типов транспортных средств.

2. Подход изготовителя транспортного средства к устранению риска сосредоточен на выявлении возможных факторов негативного воздействия на его типы транспортных средств, что приводит к детальному выяснению причины, которая может повлечь такое воздействие вследствие возможных злоумышленных действий и параметров безопасности его сетей и систем.

3. Выявление рисков изготовителем транспортных средств основано на хорошо понятных предположениях, которые строятся на современном понимании факторов, подвергающих угрозе безопасность его типов транспортных средств и его сектора.

4. Выявление рисков изготовителем транспортного средства основано на понимании факторов уязвимости его типов транспортных средств.

5. Изготовитель транспортного средства проводит детальный анализ возможных угроз и понимает, как это относится к его организации в контексте данной угрозы для его типов транспортных средств и его сектора.

P. Пункт 7.2.2.2, часть c)

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

Разъяснение требования

Цель этого требования заключается в следующем: изготовитель должен продемонстрировать процессы и правила, которые он использует для оценки, классификации и устранения выявленных рисков.

Примеры документов/доказательственных данных, которые могут быть предоставлены

В этой связи могут применяться следующие стандарты:

a) ISO/SAE 21434, в особенности на основе [RQ-08-11], [RQ-08-04], [RQ-08-06], [RQ-08-10], [RQ-08-12], [RQ-09-07], [RQ-05-06], [RQ-09-08];

b) для рассмотрения вопросов надежности и безопасности можно воспользоваться спецификацией BSI PAS 11281:2018.

В ходе используемых процессов могут быть рассмотрены следующие моменты:

c) оценка соответствующего воздействия, связанного с рисками, указанными в требовании 7.2.2.2 b);

d) выявление потенциальных путей воздействия, связанных с рисками, указанными в требовании 7.2.2.2 b);

e) определение осуществимости/вероятности противоправного воздействия по каждому из указанных выше путей противоправного воздействия;

f) расчет и классификация рисков;

g) варианты устранения выявленных и классифицированных рисков.

Данное требование следует считать невыполненным, если справедливо одно из следующих утверждений

1. Результаты оценки рисков слишком сложны или громоздки, чтобы ими могли воспользоваться директивные органы, и в этой связи их невозможно довести до их сведения четким и своевременным образом.

2. Требования безопасности и методы смягчения последствий носят произвольный характер или берутся из соответствующего контрольного каталога без учета того, каким образом они будут содействовать обеспечению безопасности данных типов транспортных средств.

3. Оформляются документально и воспринимаются только некоторые домены или типы ресурсов. Факторы зависимости между соответствующими категориями непонятны (например, зависимость между ИТ и ОТ).

4. Учетные данные ресурсов, имеющих отношение к типам транспортных средств, неполны, отсутствуют или недостаточно подробны.

5. Учетные данные ресурсов не принимаются во внимание и устарели.

6. Системы оцениваются изолированно без учета зависимостей и взаимодействий с другими системами (например, взаимодействия между ИТ- и ОТ-средой).

7. Оценка риска не строится на четко определенном наборе допущений.

8. Оценка риска для типов транспортных средств является «разовым» мероприятием (или не производится вообще).

Данное требование можно считать выполненным, если справедливы все следующие утверждения

1. Результатом процесса управления рисками изготовителем транспортных средств должен являться четкий комплекс требований к безопасности, который позволяет устранять риски в соответствии с его организационным подходом к безопасности.

2. Все ресурсы, имеющие отношение к безопасной эксплуатации его типов транспортных средств, идентифицируются и вносятся в учетную ведомость (на соответствующем уровне детализации).

3. Учетная ведомость обновляется.

4. Факторы зависимости от вспомогательной инфраструктуры выявляются и регистрируются.

5. Изготовитель транспортных средств расставляет ресурсы в порядке приоритетности в зависимости от степени их важности для эксплуатации его типов транспортных средств.

6. Выявление рисков изготовителем транспортных средств основано на хорошо понятных предположениях, которые строятся на современном понимании факторов, подвергающих угрозе безопасность его типов транспортных средств и его сектора.

7. Выявление рисков изготовителем транспортных средств основано на понимании факторов уязвимости его типов транспортных средств.

8. Изготовитель может подтвердить эффективность и воспроизводимость своих процессов в целях их классификации и учета риска.

Q. Пункт 7.2.2.2, часть d)

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

Разъяснение требования

Цель этого требования заключается в следующем: изготовитель должен продемонстрировать процессы и правила, которые он использует для принятия решения по поводу способов устранения выявленных рисков. Это может включать критерии принятия решения по управлению рисками, например посредством налаживания процесса отбора и введения в действие соответствующих средств контроля, и определение случаев, в которых придется идти на некоторый риск.

Результаты этого процесса выявления и оценки рисков следует учитывать при выборе подходящих вариантов управления этими рисками. В итоге этот процесс должен привести к тому, что остаточный риск (риск, оставшийся после принятия мер по его снижению) находится в пределах заявленных производителем допусков (т. е. в пределах заявленных приемлемых пределов).

В ходе этих процессов рассматриваются меры по снижению рисков, указанные в приложении 5 к Правилам по кибербезопасности.

Примеры документов/доказательственных данных, которые могут быть предоставлены

В этой связи могут применяться следующие стандарты:

a) в качестве основы для подтверждения и оценки работы можно воспользоваться в случае необходимости стандартом ISO/SAE 21434, в особенности на основе [RQ-09-09];

b) можно также применить стандарт ISO 31000, если он адаптирован к рискам, имеющим отношение к данному изделию.

В ходе используемых процессов могут быть рассмотрены следующие моменты:

c) надлежащие и пропорциональные методологии устранения рисков;

d) обработка критических элементов (с точки зрения безопасности и окружающей среды) с целью обеспечить такое положение, при котором уровень рисков в этом плане был бы надлежащим образом снижен и соразмерен по отношению к целям в области безопасности или охраны окружающей среды, обусловленным соответствующими системами транспортных средств;

e) обеспечение такого положения, при котором остаточный риск оставался бы для компонентов или всего типа транспортных средств в целом в приемлемых пределах;

f) детальное описание любых случаев, в которых данная организация может согласиться с обоснованием отказа от соблюдения заявленной допустимой степени риска.

Данное требование следует считать невыполненным, если справедливо одно из следующих утверждений

1. Элементы безопасности проектов или программ зависят исключительно от завершения оценки управления рисками, т. е. безотносительно к конечным результатам.

2. Отсутствует системный процесс, обеспечивающий эффективное управление выявленными рисками в области безопасности.

3. Риски, зарегистрированные в соответствующем учетном журнале, остаются не устраненными в течение длительного периода времени в ожидании принятия решений на высшем уровне или выделения ресурсов для их устранения.

Данное требование можно считать выполненным, если справедливы все следующие утверждения

1. Существенные выводы, сделанные в процессе управления рисками изготовителя транспортных средств, доводятся до сведения ключевых лиц, принимающих решения в области безопасности, и подведомственных им сотрудников.

2. Эффективность процесса управления рисками изготовителя транспортных средств подвергается периодической проверке, по результатам которой вносятся, по мере необходимости, соответствующие улучшения.

R. Пункт 7.2.2.2, часть e)

«e) процессы, используемые для проверки кибербезопасности типа транспортного средства;»

Разъяснение требования

Цель этого требования — обеспечить изготовителю соответствующие возможности и процессы для проведения испытаний типа транспортного средства на всех этапах его разработки и производства.

Процессы проверки на этапе производства могут отличаться от процессов, используемых на этапе разработки.

Примеры документов/доказательственных данных, которые могут быть предоставлены

В этой связи могут применяться следующие стандарты:

a) в качестве основы для подтверждения и оценки работы можно воспользоваться в случае необходимости стандартом ISO/SAE 21434, в особенности на основе [RQ-9-10], [RQ-10-01], [RQ-11-01], [RQ-11-02], [RQ-12-01];

b) для рассмотрения вопросов взаимодействия процессов надежности и безопасности и процессов подтверждения результатов обеспечения безопасности можно воспользоваться спецификацией BSI PAS 11281:2018.

В ходе используемых процессов могут быть рассмотрены следующие моменты:

Этап разработки:

c) конкретные правила организации, касающиеся проверок в процессе разработки;

d) процессы создания и реализации стратегий проверок;

e) процессы планирования проверки кибербезопасности;

f) процессы проверки конструкции систем кибербезопасности;

g) процессы проверки блока программного обеспечения кибербезопасности;

h) процессы проверки аппаратного обеспечения кибербезопасности;

i) процессы комплексной проверки системы кибербезопасности;

j) процессы документального оформления результатов проверки;

k) процессы работы по устранению факторов уязвимости, выявленных в ходе проверки;

l) обоснование и требования к проверкам системы кибербезопасности, таким как функциональная проверка (на основе действующих требований, на наличие и отсутствие неполадок), проверка интерфейса, проверка на проникновение, сканирование на уязвимость, случайное тестирование, но не ограничивающееся одной и той же позицией.

Этап реализации:

m) процессы проверки с целью убедиться в том, что в создаваемой системе заложены соответствующие требования, функции контроля и возможности в области кибербезопасности, изложенные в производственном плане;

n) процессы проверки с целью убедиться в том, что изготовляемый компонент удовлетворяет спецификациям кибербезопасности, которые соответствуют системе на этапе разработки;

o) процессы проверки с целью убедиться в том, что устройства обеспечения и конфигурации системы кибербезопасности в качестве спецификаций кибербезопасности в производимом изделии активированы;

p) процессы документального оформления результатов тестирования и проработки выводов.

Данное требование следует считать невыполненным, если справедливо одно из следующих утверждений

1. Конкретный продукт или услуга рассматривается как «единственно правильное решение», и в этой связи утверждения изготовителя принимаются как данность.

2. Методы гарантии применяются без оценки их преимуществ и недостатков, таких как риски в случае тестирования на проникновение в условиях эксплуатации.

3. Гарантии действует по той причине, что никаких известных проблем на данный момент не было.

Данное требование можно считать выполненным, если справедливы все следующие утверждения

1. Изготовитель транспортного средства подтверждает, что меры безопасности, применяемые для защиты систем, являются эффективными и действуют до окончания срока службы всех транспортных средств, относящихся к тем типам транспортных средств, для которых они необходимы.

2. Изготовитель транспортного средства понимает доступные ему методы обеспечения достоверности и выбирает те из них, которые позволяют ему испытывать чувство доверия к безопасности своих типов транспортных средств.

3. Доверие изготовителя данного транспортного средства к безопасности в части его технологии, людей и процессов может быть обосновано и проверено третьей стороной.

4. Недостатки в области безопасности, выявленные в ходе мероприятий, связанных обеспечением гарантий, оцениваются, классифицируются в порядке приоритетности и при необходимости своевременно и эффективно устраняются.

5. Методы, используемые для обеспечения гарантий, пересматриваются с целью убедиться в том, что они работают, как положено, и остаются самым подходящим методом, который следует использовать и впредь.

S. Пункт 7.2.2.2, часть f)

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

Разъяснение требования

Цель этого требования — обеспечить актуальность оценки рисков. Это требование должно включать процессы, позволяющие выяснить, изменились ли риски в случае того или иного типа транспортного средства и как это будет учитываться в рамках оценки рисков.

Источники, подлежащие идентификации риска, могут указываться. Они могут включать:

a) платформы обмена информацией о факторах уязвимости/угрозах;

b) уроки, извлеченные в связи с соответствующими рисками и факторами уязвимости;

c) совещания.

Следует отметить, что требования 7.2.2.2, части f)–h), могут перекрываться с точки зрения используемых процессов и в этой связи одни и те же доказательства могут быть применимы для доказательства выполнения и этих требований.

Примеры документов/доказательственных данных, которые могут быть предоставлены

d) в качестве основы для подтверждения и оценки работы можно воспользоваться в случае необходимости стандартом ISO/SAE 21434, в особенности на основе [RQ-11-3], [RQ-6-8], [RQ-07-05], [RQ-07-06].

Данное требование следует считать невыполненным, если справедливо одно из следующих утверждений

1. Процессов, требующих обновления оценки рисков, не существует.

Данное требование можно считать выполненным, если справедливы все следующие утверждения

1. Изготовитель транспортного средства проводит оценку рисков в том случае, когда на типах транспортных средств могут сказаться такие значительные события, как замена системы или изменение угрозы кибербезопасности.

2. Оценки рисков, производимые изготовителем транспортных средств, носят динамичный характер и обновляются в свете соответствующих изменений, которые могут включать техническую модификацию типов транспортных средств, изменение условий эксплуатации и новую информацию, касающуюся угроз.

T. Пункт 7.2.2.2, часть g)

«g) процессы, используемые для мониторинга, обнаружения и реагирования на кибератаки, киберугрозы и уязвимости соответствующих типов транспортных средств и процессов, используемых для оценки того, являются ли принимаемые меры кибербезопасности по-прежнему эффективными в свете новых киберугроз и факторов уязвимости, которые были выявлены;»

Разъяснение требования

Цель этого требования — обеспечить такое положение, в случае которого изготовитель располагал бы соответствующими процессами для отслеживания кибератак, угроз или факторов уязвимости в отношении транспортных средств, которые были официально утверждены по просьбе изготовителя, т. е. находятся на этапе после производства или на этапе производства, а также наладил бы процессы, позволяющие ему реагировать в этой связи надлежащим и своевременным образом.

Следует отметить, что требования 7.2.2.2, части f)–h), могут перекрываться с точки зрения используемых процессов и в этой связи одни и те же доказательства могут быть применимы для доказательства выполнения и этих требований.

Примеры документов/доказательственных данных, которые могут быть предоставлены

Могут применяться следующие стандарты:

a) в качестве основы для подтверждения и оценки работы можно воспользоваться в случае необходимости стандартом ISO/SAE 21434, в особенности на основе [RQ-07-01], [RQ-07-02], [RQ-07-03], [RQ-07-04], [RQ-07-05], [RQ-15-04], [RQ-15-05], [RC-15-03], [RQ-13-01], [RQ-13-02], [RQ-13-03].

Нижеследующие положения могут быть использованы для подтверждения используемых процессов:

b) процессы мониторинга кибербезопасности транспортных средств на этапе после их изготовления. Это может включать процессы сбора информации, которая может иметь или не иметь отношения к данному транспортному средству/данной системе изготовителя;

c) процессы оценки информации по кибербезопасности. Речь идет о процессах определения уместности собранной информации, касающейся системы/транспортного средства изготовителя;

d) процессы определения/оценки рисков применительно к требуемой информации;

e) процедуры реагирования на дорожно-транспортные происшествия как для уже зарегистрированных, так и для еще не зарегистрированных типов транспортных средств, подпадающих под действие СОКиБ, которые могут включать подтверждение процедур в случае:

i) взаимодействия с компетентными органами;

ii) выявленных или подтвержденных факторов, которые могут явиться причиной нарастания проблем или необходимости соответствующих действий;

iii) определения вариантов ответных действий и условий, в которых их можно предпринять;

iv) урегулирования любых факторов зависимости и взаимодействия с поставщиками;

f) подтверждение того, что процедуры реагирования будут работать, например посредством проведения тренировок и проверок с целью убедиться в том, что предположения, на которых строилась система планирования, подтверждают свою актуальность в ходе испытаний.

Данное требование следует считать невыполненным, если справедливо одно из следующих утверждений

1. У изготовителя данного транспортного средства нет источников, которые указывали бы на наличие угрозы.

2. После получения обновлений изготовитель транспортного средства не применяет их своевременно.

3. Изготовитель транспортного средства не оценивает полезность своей информации, касающейся угроз, и не делится ею с поставщиками, уполномоченными предприятиями, которые занимаются послепродажным обслуживанием, или другими пользователями.

4. Нет сотрудников, которые выполняли бы функцию мониторинга.

5. У сотрудников по мониторингу нет нужных профессиональных навыков.

6. Сотрудники по мониторингу не способны представить отчеты в соответствии с требованиями руководства.

7. Сигналы, указывающие на угрозу безопасности в случае тех или иных типов транспортных средств, не классифицируются по приоритетности.

Данное требование можно считать выполненным, если справедливы все следующие утверждения

1. Производится сбор данных, касающихся безопасности и эксплуатации соответствующих типов транспортных средств.

2. Сигналы тревоги, поступающие от третьих сторон, расследуются, и принимаются соответствующие меры.

3. Некоторые наборы данных можно легко вызвать с помощью поисковых систем, используемых в целях оказания помощи в изысканиях.

4. Реагирование на сигналы тревоги в отношении того или иного ресурса или системы производится регулярно.

5. Сигналы, указывающие на угрозу безопасности в случае тех или иных типов транспортных средств, классифицируются по приоритетности.

6. Изготовитель транспортного средства своевременно подает заявки на обновление.

7. У изготовителя транспортных средств действуют процессы мониторинга, обнаружения и реагирования в случае кибератак, киберугроз и факторов уязвимости, которые имеют отношение к его коммерческим потребностям или конкретным угрозам в его секторе.

8. Изготовитель транспортных средств осведомлен, насколько эффективны его процессы (например, посредством отслеживания того, как они помогают ему выявлять проблемы, связанные с безопасностью).

9. Сотрудники, занимающиеся мониторингом, обладают надлежащими навыками проведения расследований и базовым пониманием данных, с которыми они должны работать.

10. Сотрудники, занимающиеся мониторингом, могут представлять отчеты другим подразделениям организации (например, руководителям подразделений по безопасности, менеджерам по вопросам устойчивости).

11. Изготовитель транспортных средств успешно освещает процессы, позволяющие выяснить, являются ли принимаемые меры по обеспечению кибербезопасности достаточно надежными и можно ли в этой связи сделать вывод о том, что они по-прежнему эффективны.

U. Пункт 7.2.2.2, часть h)

«h) процессы, используемые в целях получения соответствующих данных, необходимых для поддержки анализа предпринятых попыток проведения кибератак или успешных кибератак;»

Разъяснение требования

Цель этого требования — обеспечить налаживание соответствующего процесса сбора данных, необходимых для анализа и связанных с этим обязанностей по работе с данными и анализу.

a) В качестве основы для подтверждения и оценки работы можно воспользоваться в случае необходимости стандартом ISO/SAE 21434, в особенности на основе [RQ-07-03].

Примеры документов/доказательственных данных, которые могут быть предоставлены

Для подтверждения используемых процессов можно использовать нижеследующие положения:

b) порядок осуществления деятельности группы реагирования на инциденты в области безопасности (инциденты);

c) мониторинг на местах (получение информации об инцидентах и факторах уязвимости);

d) процедура, когда происходит инцидент (включая обзор информации, которая передается специалисту по анализу и на каких этапах);

e) процедура, когда выявляется соответствующий фактор уязвимости (включая обзор информации, которая передается специалисту по анализу и на каких этапах).

V. Пункт 7.2.2.3

«7.2.2.3 Изготовитель транспортного средства подтверждает, что процессы, используемые в его системе обеспечения кибербезопасности, будут обеспечивать — на основе классификации, указанной в пунктах 7.2.2.2 c) и 7.2.2.2 g), — снижение уровня киберугроз и факторов уязвимости, которые предполагают соответствующие меры реагирования со стороны изготовителя этого транспортного средства в разумные сроки».

Разъяснение требования

Цель этого требования — обеспечить налаживание, после идентификации выявленных рисков, соответствующего процесса определения сроков реагирования на основе результатов классификации.

В этой связи необходимо установить крайний срок реагирования в рамках таких процессов, как сортировка, и разъяснить процесс мониторинга с целью убедиться в том, что он укладывается в установленные сроки.

Сроки, установленные изготовителями, должны быть такими, чтобы их можно было обосновать и объяснить. Можно предусмотреть соответствующий набор временны́х диапазонов, охватывающих различные возможные ситуации. Он должен включать временны́е диапазоны для принятия решений и реализации возможных мер реагирования или ответных мер.

В качестве основы для подтверждения и оценки работы можно воспользоваться в случае необходимости стандартом ISO/SAE 21434, в особенности на основе [RQ-05-02] b).

Примеры документов/доказательственных данных, которые могут быть предоставлены

Нижеследующие положения могут быть использованы для подтверждения используемых процессов:

a) порядок осуществления деятельности по реагированию на инциденты в области кибербезопасности, включая:

i) мониторинг на местах (получение информации об инцидентах и факторах уязвимости);

ii) процедура урегулирования инцидентов, включая методы определения сроков реагирования;

iii) процедуры обнаружения факторов уязвимости;

b) демонстрация методов выполнения таких процедур.

W. Пункт 7.2.2.4

«7.2.2.4 Изготовитель транспортного средства подтверждает, что процессы, используемые в его системе обеспечения кибербезопасности, будут обеспечивать мониторинг, указанный в пункте 7.2.2.2 g), на постоянной основе. Они включают:

a) транспортные средства после первой регистрации в системе мониторинга;

b) возможности анализа и обнаружения киберугроз, факторов уязвимости и кибератак на основе данных о транспортном средстве и журналов учета использования транспортного средства. Эти возможности используются с соблюдением пункта 1.3 и права владельцев или водителей автомобилей на неприкосновенность частной жизни, особенно в том, что касается согласия».

Разъяснение требования

Цель данного требования — обеспечить непрерывность процессов мониторинга кибератак, киберугроз и факторов уязвимости на типах транспортных средств и их применения ко всем зарегистрированным транспортным средствам данного изготовителя, на которые распространяется действие их системы управления кибербезопасностью, и использования в этих целях:

a) информации о мониторинге, полученной в соответствии с пунктом 7.3.7, в дополнение к другим источникам информации о мониторинге, полученной в соответствии с пунктом 7.2.2.2 g) (например, по социальным сетям).

Следует отметить, что особое отношение к этому требованию имеет пункт 1.3 и соблюдение законов о конфиденциальности данных.

В качестве основы для доказательства и оценки можно использовать по мере необходимости стандарт ISO/SAE 21434, в особенности в случае разделов 7.3 «Мониторинг кибербезопасности», 7.4 «Оценка событий в области кибербезопасности», 7.5 «Анализ факторов уязвимости».

Примеры документов/доказательственных данных, которые могут быть предоставлены

Нижеследующие положения могут быть использованы для подтверждения используемых процессов:

b) порядок осуществления деятельности по реагированию на инциденты в области кибербезопасности, включая:

i) мониторинг на местах (получение информации об инцидентах и факторах уязвимости);

ii) процедура урегулирования инцидентов;

iii) процедуры обнаружения факторов уязвимости;

c) демонстрация методов выполнения таких процедур.

X. Пункт 7.2.2.5

«7.2.2.5 Изготовитель транспортного средства должен продемонстрировать, каким образом его система обеспечения кибербезопасности будет регулировать соответствующие аспекты взаимозависимости, которая может быть налажена у него с поставщиками изделий и услуг, с которыми заключены соответствующие контракты, или с его подрядными организациями в связи с требованиями пункта 7.2.2.2».

Разъяснение требования

Цель этого требования — показать, что риски со стороны поставщиков могут быть известны и управляться в рамках процессов, описанных в СОКиБ. Принимаемые меры должны быть соразмерны рискам, связанным с тем, что поставляется.

Окончательное осуществление этих процессов может быть включено в соответствующее двустороннее соглашение между изготовителем транспортного средства и его поставщиками.

В рамках СОКиБ могут использоваться процессы, предусматривающие:

a) выявление рисков, связанных с частями, компонентами, системами или услугами, предоставляемыми поставщиками;

b) управление рисками применительно к транспортному средству со стороны поставщиков услуг, выполняющих функции подключения или оказывающих услуги, от которых зависит работа транспортного средства, включая, например, поставщиков «облачных технологий», поставщиков телекоммуникационных услуг, поставщиков интернет-услуг и уполномоченных поставщиков послепродажного обслуживания;

c) обеспечение возможности, позволяющей подрядчикам и/или поставщикам услуг доказать, каким образом они управляли связанными с ними рисками. Эти процессы могут включать анализ требований по подтверждению или проверке, которые могут быть использованы в порядке доказательства того факта, что риски устраняются надлежащим образом;

d) передачу соответствующих требований соответствующим отделам или подрядным организациям изготовителя для управления выявленными рисками.

Следует отметить, что соответствующие требования можно предъявлять к поставщикам 1-го уровня и требовать, чтобы они возлагали их на поставщиков 2-го уровня. Вместе с тем изготовителю может быть трудно переложить свою ответственность в случае этих требований дальше по цепочке поставок (особенно юридически обязательные требования).

Примеры документов/доказательственных данных, которые могут быть предоставлены

Могут применяться следующие стандарты:

e) в качестве основы для подтверждения и оценки работы можно воспользоваться в случае необходимости стандартом ISO/SAE 21434, в особенности на основе [RQ-06-09], [RQ-15-03], [RQ-15-02].

Нижеследующие положения могут быть использованы для подтверждения используемых процессов:

f) действующие договорные соглашения или данные, подтверждающие такие соглашения;

g) подтвержденные аргументы в пользу того, каким образом их процессы обеспечат учет поставщиков/провайдеров услуг в процессе оценки рисков;

h) процедуры/методы обмена информацией о рисках между поставщиками и изготовителями;

i) в целях подтверждения можно использовать существующие решения/ контракты, такие как правила СУИБ (система управления информационной безопасностью). Это можно подтвердить с помощью сертификатов, выдаваемых на основе стандарта ISO/IEC 27001 или системы TISAX (Система надежного обмена оценками информационной безопасности).

Данное требование следует считать невыполненным, если справедливо одно из следующих утверждений

1. Соответствующие договоры с поставщиками и провайдерами услуг не содержат требований к кибербезопасности.

Данное требование можно считать выполненным, если справедливы все следующие утверждения

1. Изготовители транспортных средств хорошо понимают свою цепочку поставок, включая субподрядчиков, и риски, с которыми они сталкиваются в более широком смысле. Изготовитель транспортных средств учитывает такие факторы, как партнерские отношения с поставщиком, конкуренция, национальная принадлежность и другие организации, с которыми он заключает договор субподряда. Это служит информационной базой для оценки рисков и процессов закупок.

2. Подход изготовителя транспортных средств к управлению рисками в цепочке поставок, строится на системе учета рисков для его типов транспортных средств, связанных с подрывной деятельностью способных и обеспеченных достаточными ресурсами злоумышленников.

3. Изготовитель транспортных средств уверен в том, что информация, необходимая для эксплуатации ваших транспортных средств, передается поставщикам и защищена от атак с применением новейших средств.

4. Изготовитель транспортного средства может четко изложить свои требования в области безопасности, которые он перекладывает на поставщиков таким образом, чтобы это было понятно на взаимной основе и закреплено в соответствующих договорах. В этом плане существует четкая и документально оформленная модель совместной ответственности.

5. Вся система сетевых подключений и обмена данными с третьими сторонами управляется эффективно и пропорционально.

6. В соответствующих случаях процесс разрешения инцидента, осуществляемый изготовителем транспортного средства, и процесс разрешения инцидента, осуществляемый его поставщиками, способствуют урегулированию таких инцидентов на взаимной основе.

Y. Пункты 7.3–7.3.1

«7.3 Требования, предъявляемые к типам транспортных средств

7.3.1 Изготовитель должен иметь действующее свидетельство о соответствии системы обеспечения кибербезопасности, относящееся к официально утверждаемому типу транспортного средства.

Однако в случае официальных утверждений типа до 1 июля 2024 года, если изготовитель транспортного средства может продемонстрировать, что данный тип транспортного средства не мог быть разработан в соответствии с СОКиБ, то этот изготовитель транспортного средства должен продемонстрировать, что на этапе разработки данного типа транспортного средства фактор кибербезопасности был учтен должным образом».

Разъяснение требования

Цель этого требования — обеспечить наличие действительного свидетельства о соответствии СОКиБ, позволяющего предоставлять официальное утверждение типа любого нового типа транспортного средства, и его соответствие данному типу транспортного средства.

В этой связи необходимо принять к сведению следующее уточнение:

a) «относящееся к официально утверждаемому типу транспортного средства» означает, что СОКиБ должна применяться к официально утверждаемому типу транспортного средства.

Примеры документов/доказательственных данных, которые могут быть предоставлены

Для доказательства действительности свидетельства СОКиБ можно использовать следующие документы:

b) свидетельство о соответствии СОКиБ с целью подтвердить, что оно все еще действительно;

c) подтверждение того факта, что СОКиБ надлежащим образом применяется к данному типу транспортного средства и любой информации, необходимой для обеспечения гарантии.

Z. Пункт 7.3.2

«7.3.2 Изготовитель транспортного средства идентифицирует применительно к официально утверждаемому типу транспортного средства те риски, которые связаны с поставщиками, и управляет этими рисками».

Разъяснение требования

Это требование конкретно касается получения достаточной информации из цепи поставок и увязано с пунктом 7.2.2.5. Цель этого требования — обеспечить достаточность представленной информации (вместе с информацией со стороны изготовителя) для проведения оценки выполнения требований, указанных в пунктах 7.3.3–7.3.6.

В этой связи необходимо принять к сведению следующее уточнение:

a) «риски, связанные с поставщиками» — цель в данном случае заключается в подтверждении того, что риски, связанные с поставщиками, могут быть известны и что ими можно управлять. Принято считать, что передача требований вниз по цепочке поставок за пределы поставщиков 2-го уровня и при этом обеспечить их юридически обязательный характер, сопряжена с трудностями.

Примеры документов/доказательственных данных, которые могут быть предоставлены

В этой связи могут применяться следующие стандарты:

b) ISO/SAE 21434.

Нижеследующие положения могут быть использованы для подтверждения процессов:

c) доказательство в форме разделов договора с поставщиками, которые касаются соответствующих требований настоящих Правил.

AA. Пункт 7.3.3

«7.3.3 Изготовитель транспортного средства идентифицирует критические элементы данного типа транспортных средств и проводит исчерпывающую оценку рисков для данного типа транспортных средств, а также надлежащим образом обрабатывает выявленные риски/управляет ими. При оценке рисков учитываются отдельные элементы типа транспортного средства и их взаимодействия. В ходе оценки рисков учитываются, кроме того, взаимодействия с любыми внешними системами. При оценке рисков изготовитель транспортного средства учитывает риски, связанные со всеми угрозами, указанными в части A приложения 5, а также любой другой соответствующий риск».

Разъяснение требования

Цель этого требования — обязать изготовителей транспортных средств определять критические элементы того или иного типа транспортных средств с точки зрения кибербезопасности и представить обоснование того, каким образом осуществляется управление связанными с ними рисками.

Изготовитель должен быть в состоянии обосновать причину, по которой он определил элементы того или иного типа транспортного средства в качестве критически важных (или не критически важных).

В этой связи необходимо принять к сведению следующее уточнение:

a) критически важными элементами могут считаться элементы, способствующие повышению уровня безопасности транспортного средства, охраны окружающей среды или защиты от угона. Они могут быть теми частями, которые выполняют функцию их подключения. Они могут также являться частями архитектуры данного транспортного средства, которые имеют решающее значение для обмена информацией или обеспечения кибербезопасности (например, в качестве критически важных могут также считаться межсетевые интерфейсы);

b) цель этого требования — обеспечить надлежащий анализ рисков/управление ими путем учета всех угроз, включая часть A приложения 5, и выяснение необходимости принятия контрмер на основе результатов анализа рисков и их оценки;

c) это требование также имеет целью дать изготовителю транспортного средства возможность продемонстрировать применение соответствующего процесса с учетом требований, содержащихся в разделах 7.2.2.2 и 7.2.2.4 СОКиБ, к данному типу транспортного средства;

d) орган по официальному утверждению или техническая служба должны ссылаться на приложение 5 к Правилам по кибербезопасности с целью помочь им удостовериться в объективности оценки риска, сделанной изготовителем;

e) в ходе рассмотрения рисков необходимо учитывать требования пункта 7.3.4 и требование, касающееся соразмерного смягчения последствий;

f) рассмотрение угроз и мер по смягчению их последствий в приложении 5 в рамках оценки рисков может привести к тому, что этим рискам будут присваивать такие рейтинги, как «неактуальные» или «незначительные».

Примеры документов/доказательственных данных, которые могут быть предоставлены

В этой связи могут применяться следующие стандарты:

g) ISO/SAE 21434 описывает способ определения данной концепции. Это также включает учет критических элементов, обусловленных решениями, которые имеют отношение к регулированию рисков. Эти результаты документально отражены в разделах «Задачи в области кибербезопасности» и «Концепция кибербезопасности». Дополнительное описание исчерпывающей оценки риска содержится в пункте 8 «Методы оценки риска». Это документально отображено в разделе «Анализ угроз и оценка рисков»;

h) ETSI TS 103 645 можно использовать для подтверждения безопасности элементов транспортного средства применительно к концепции «Интернет вещей»;

i) можно использовать спецификацию BSI PAS 1885.

Для подтверждения используемых процессов можно использовать нижеследующие положения:

j) запрос данных, касающихся типа транспортного средства;

k) разъяснение причин, по которым те или иные элементы, относящиеся к данному типу транспортного средства, являются критическими;

l) какие меры безопасности введены в действие, включая информацию о том, как они работают;

m) информация о любых мерах безопасности должна позволять технической службе/органу по официальному утверждению, быть уверенными в том, что они делают именно то, что предусмотрено изготовителем, и что на транспортных средствах в процессе производства будет использоваться та же мера, которая была доведена до сведения органа по официальному утверждению/технической службе в

отношении данного типа транспортного средства. Конфиденциальность конкретных данных и порядок обращения с ними должны согласовываться и регистрироваться.

AB. Пункт 7.3.4

«7.3.4 Изготовитель транспортного средства предохраняет данный тип транспортного средства от рисков, выявленных в ходе оценки рисков изготовителем транспортного средства. В целях предохранения данного типа транспортного средства принимаются соразмерные меры по смягчению последствий. Осуществляемые меры по смягчению последствий включают все меры по смягчению последствий, о которых говорится в частях B и C приложения 5 и которые касаются выявленных рисков. Однако, если та или иная мера по смягчению последствий, упомянутая в части B или C приложения 5, не имеет отношения к выявленному риску или является недостаточной, изготовитель транспортного средства обеспечивает осуществление какой-либо иной соответствующей меры по смягчению последствий.

В частности, в случае официальных утверждений типа до 1 июля 2024 года, изготовитель транспортного средства обеспечивает осуществление какой-либо иной соответствующей меры по смягчению последствий, если та или иная мера по смягчению последствий, упомянутая в части B или C приложения 5, технически неосуществима. Соответствующая оценка технической осуществимости представляется изготовителем органу по официальному утверждению».

Разъяснение требования

Цель этого требования — обеспечить, чтобы изготовители транспортных средств принимали соответствующие меры по снижению риска в соответствии с результатами оценки рисков.

Изготовитель должен представить аргументированные доводы и доказательства в пользу уменьшения воздействия на окружающую среду, которыми они руководствовались в процессе разработки данного типа транспортного средства, а также объяснить, почему они являются достаточными. Это может включать любые допущения, например взаимодействие внешних систем с транспортным средством.

Технические меры смягчения последствий, указанные в частях B и C приложения 5, рассматриваются в тех случаях, когда это применимо к рискам, которые необходимо смягчить. Изготовитель может представить обоснование не только тех мер смягчения, которые указаны в приложении 5 как «не имеющие отношения или недостаточные», но и того довода, что иная мера по смягчению последствий (помимо тех, которые перечислены в приложении 5) соответствует данному конкретному риску. Это обоснование может быть подтверждено оценкой рисков и рейтингом рисков, показывающим целесообразность альтернативного смягчения последствий. Это позволит ввести в практику новые или усовершенствованные технологии защиты.

В этой связи необходимо принять к сведению следующее уточнение:

a) проектные решения изготовителя необходимо увязывать со стратегией оценки рисков и управления рисками. Изготовитель должен быть в состоянии обосновать ту стратегию, которую он использовал;

b) термин «соразмерный» следует учитывать в процессе выбора требуемых вариантов: следует ли осуществлять смягчение последствий и какие именно меры следует принимать. Если данным видом риска можно пренебречь, то можно утверждать, что уменьшать его нет необходимости;

c) защита от выявленных рисков означает снижение данного риска.

Примеры документов/доказательственных данных, которые могут быть предоставлены

В этой связи могут применяться следующие стандарты:

d) ISO/SAE 21434 описывает порядок идентификации риска и выведенные методом дедукции цели и соответствующую концепцию кибербезопасности на основе идентифицированных рисков. Эти результаты документально отражены в частях [WP-09-04] «Задачи в области кибербезопасности» и [WP-09-07] «Концепция кибербезопасности»;

e) для обоснования конструкторских решений изготовителя можно использовать спецификацию BSI PAS 11281:2018 и другие стандарты, касающиеся претензий, аргументов и доказательств.

Для подтверждения обоснованности мер по смягчению последствий можно использовать нижеследующие положения:

f) подтверждение того, что меры по смягчению последствий были введены в силу необходимости; это включает следующее:

i) причина, если принимаются другие меры по смягчению последствий, отличные от тех, которые предусмотрены в приложении 5 (части B и C);

ii) причина, если не принимаются меры по смягчению последствий, перечисленные в приложении 5;

iii) причина, если будет установлено, что в мерах по смягчению последствий нет нужды.

AC. Пункт 7.3.5

«7.3.5 Изготовитель транспортного средства принимает надлежащие и соразмерные меры для обеспечения безопасности специальных объектов (если таковые предусмотрены) в целях хранения и реализации программного обеспечения, услуг, приложений или данных в интересах вторичного рынка применительно к данному типу транспортного средства».

В этой связи необходимо принять к сведению следующее уточнение:

a) «надлежащие и соразмерные меры» означают, что производитель должен быть в состоянии обосновать, каким образом осуществляется управление рисками, связанными с любой особой средой, которая определена в его оценке рисков;

b) особая среда может создаваться на транспортном средстве. Если транспортное средство взаимодействует с серверами или службами, расположенными вне транспортного средства (например, в «облаке»), то в этом случае следует учитывать те риски, которые они создают для данного транспортного средства с точки зрения их кибербезопасности.

Примеры документов/доказательственных данных, которые могут быть предоставлены

В этой связи могут применяться следующие стандарты:

c) в стандарте ISO/SAE 21434 описаны основные этапы соответствующего процесса, позволяющие сделать вывод об используемой архитектуре. Этот аспект следует учитывать в сценариях угроз [WP-08-03].

Для подтверждения используемых процессов можно использовать нижеследующие положения:

d) описание особой среды;

e) какие меры безопасности введены в действие, включая информацию о том, как они работают;

f) информация о любых мерах безопасности должна позволять органу по официальному утверждению/технической службе, быть уверенными в том, что они выполняют ту функцию, которую предусмотрел изготовитель, и что на транспортных средствах в процессе производства будут использоваться те же меры, которые были представлены органу по официальному утверждению/технической службе в отношении данного типа транспортного средства. Конфиденциальность конкретных данных и порядок обращения с ними должны быть согласованы и зарегистрированы;

g) см. приложение 5 к Правилам по кибербезопасности.

AD. Пункт 7.3.6

«7.3.6 До официального утверждения типа изготовитель транспортного средства проводит надлежащие и достаточные испытания в целях проверки эффективности принятых мер защиты».

Разъяснение требования

На момент официального утверждения типа результаты испытаний должны быть приемлемыми. Техническая служба может провести испытания на безопасность для подтверждения этих результатов.

В этой связи необходимо принять к сведению следующее уточнение:

a) целью любых мер безопасности является снижение рисков. Проверка должна подтвердить обоснованность принимаемых меры безопасности.

Примеры документов/доказательственных данных, которые могут быть предоставлены

В этой связи могут применяться следующие стандарты:

b) изготовители могут описать меры проверки и валидации, принятые в соответствии с ISO/SAE 21434, часть [WP-09-08] «Отчет о проверке концепции кибербезопасности», часть [WP-10-03] «Отчет о проверке уточненной спецификации кибербезопасности», часть [WP-11-02] «Отчет о валидации».

Для подтверждения используемых процессов можно использовать нижеследующие положения:

c) что проверяется и по какой причине (например, каким образом выглядят показатели успешного проведения проверки);

d) используемая методология и по какой причине (например, это может включать примечания с уточнением масштабов проверки и выполненной в ее процессе работы);

e) кто и почему проводил проверки (например, на своем предприятии, у поставщика или во внешней организации, а также любая соответствующая информация, касающаяся их квалификации/опыта);

f) подтверждение успешного результата проверки (это может включать критерии «прошла/не прошла» и результат проверки).

AE. Пункт 7.3.7

«7.3.7 Изготовитель транспортного средства принимает в отношении данного типа транспортного средства соответствующие меры в целях:

a) обнаружения и предотвращения кибератак на транспортные средства данного типа;

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

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

Разъяснение требования

Цель данного требования — обеспечить принятие конкретных мер для данного типа транспортных средств в целях отслеживания изменений в системе угроз, обнаружить и предотвратить кибератаки, а также иметь возможность провести криминалистическую экспертизу любой попытки или успешной атаки.

В этой связи необходимо принять к сведению следующее уточнение:

a) меры в связи с этим положением можно принимать непосредственно на данном типе транспортного средства или в условиях его эксплуатационной среды, например на внутреннем сервере, в мобильной сети «для данного типа транспортного средства»;

b) меры должны быть направлены в первую очередь на предотвращение успешных кибератак со ссылкой на пункты 7.3.4 и 7.3.5 для защиты от рисков, выявленных в ходе оценки рисков;

c) меры по предотвращению успешных кибератак на все транспортные средства того или иного типа могут дополнительно осуществляться асинхронно, т. е. после фактического эпизода кибератаки и его анализа;

d) возможности криминалистической экспертизы данных могут включать возможность предоставления и анализа учетных данных, диагностических кодов ошибок, информации, касающейся эксплуатационных данных транспортных средств, и информации, снимаемой с внутренних серверов в целях расследования кибератак;

e) возможности криминалистической экспертизы данных могут включать проверку кольцевого буфера сохраняющихся учетных данных, что позволит облегчить следственные процедуры.

Следует отметить, что особое отношение к этому требованию имеет пункт 1.3 и соблюдение законов о конфиденциальности данных.

Примеры документов/доказательственных данных, которые могут быть предоставлены

В этой связи могут применяться следующие стандарты:

f) ISO/SAE 21434. Перечень источников для мониторинга кибербезопасности приведен в пункте 7.3. Результаты анализа и порядок его документального оформления описаны в [WP-07-04] — Анализ уязвимости.

В целях подтверждения используемых процессов можно использовать нижеследующие принципы:

g) меры по предотвращению атаки, применяемые к данному типу транспортного средства;

h) демонстрация проведения превентивных мероприятий и мониторинга того или иного типа транспортного средства;

i) демонстрация проведения криминалистической экспертизы.

AF. Пункт 7.3.8

«7.3.8 Криптографические модули, используемые для целей настоящих Правил, должны соответствовать согласованным стандартам. Если используемые криптографические модули не соответствуют согласованным стандартам, то изготовитель транспортного средства должен обосновать их использование».

В этой связи необходимо принять к сведению следующее уточнение:

Согласованный стандарт может быть международно признанным или национальным стандартом, который находит широкое применение, например ФИПС.

Разъяснение требования

Цель этого требования — обеспечить обоснованность используемых методов шифрования.

Примеры документов/доказательственных данных, которые могут быть предоставлены

В случае применения мер шифрования, основанных на результатах анализа и оценки рисков, изготовитель должен быть в состоянии:

a) объяснить, соответствует ли алгоритм или способ шифрования действующему согласованному стандарту; и

b) объяснить причину выбора данного вида шифрования и почему оно адекватно снижает выявленный риск.

AG. Пункт 7.4

«7.4 Положения об отчетности

7.4.1 Изготовитель транспортного средства предоставляет по меньшей мере один раз в год или чаще, если это необходимо, органу по официальному утверждению или технической службе отчет о результатах своей деятельности по мониторингу, как она определена в подпункте g) пункта 7.2.2.2, который должен включать соответствующую информацию о новых кибератаках. Изготовитель транспортного средства также сообщает и подтверждает органу по официальному утверждению или технической службе, что меры по смягчению последствий рисков для кибербезопасности, применяемые в отношении его типов транспортных средств, по-прежнему эффективны, а также любые дополнительные меры, принятые в этой связи».

Разъяснение требования

Основная цель этого требования — подтвердить, что аспекты СОКиБ, связанные с мероприятиями по мониторингу кибербезопасности, как они определены в пункте 7.2.2.2 g), по-прежнему применяются надлежащим образом после завершения этапа разработки и что соответствующие меры по смягчению последствий рисков для кибербезопасности, принятые в этой области, продолжают оставаться эффективными.

Изготовитель не реже одного раза в год представляет отчет органу по официальному утверждению типа или технической службе, которые проверяли соответствие его СОКиБ настоящим Правилам. Если наблюдаются такие случаи, как новые кибератаки, то эти отчеты следует представлять чаще, прежде всего для того, чтобы сообщить о любых предпринятых действиях.

Примеры документов/доказательственных данных, которые могут быть предоставлены

В этой связи могут применяться следующие стандарты:

a) ISO/SAE 21434, в котором содержатся следующие определения: часть [WP-07-02] «Результаты сортировки информации о кибербезопасности» и часть [WP-07-04] «Анализ уязвимости». Оба эти определения можно использовать для требуемой отчетности в качестве исходных данных.

AH. Пункт 7.4.2

«7.4.2 Орган по официальному утверждению или техническая служба проверяет представленную информацию и в случае необходимости требует от изготовителя транспортного средства устранить любой выявленный фактор неэффективности.

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

Никаких руководящих указаний в отношении этого требования в настоящий документ внесено не было.

AI. Пункт 8

«8. Модификация и распространение официального утверждения типа транспортного средства»

Примеры документов/доказательственных данных, которые могут быть предоставлены

В нижеследующей таблице приводятся некоторые примеры изменений архитектуры E/E и потенциального воздействия на тип данного транспортного средства в связи с настоящими Правилами.

Просьба принять к сведению тот факт, что приведенные примеры указывают лишь на то, что можно принять во внимание, но что нельзя рассматривать как ограничение. Если воспользоваться приведенным примером изменений, то ожидаемый результат может оказаться иным.

	Возможные **изменения** в архитектуре E/E	Воздействие на тип	Примеры
Новый тип	**Разработка новой архитектуры E/E**	Разработка архитектуры E/E предполагает необходимость **нового типа**	Разработка архитектуры E/E предполагает необходимость **нового типа**
Новый тип	**Изменение результатов оценки рисков вследствие использования новых технологий**	Нуждается в новом типе, так как безопасность существующей подсистемы подвергается воздействию	• Добавление новых внешних интерфейсов (NFC — ближняя бесконтактная связь) для новых услуг, таких как персонализация • Изменение топологии сети путем добавления нового шлюза
Распространение существующего типа	**Незначительные изменения в итоговой оценке рисков путем добавления или замены подсистем**	Замена существующей подсистемы или добавление новой подсистемы, что вносит некоторые незначительные изменения в кибербезопасность результирующей архитектуры E/E и, следовательно, предполагает необходимость распространения типа	• Замена коммуникационного блока UMTS на коммуникационный блок 5G –> возможна дополнительная связь • Замена ЭБУ на новый модуль с HSM (аппаратный модуль безопасности)
Без изменений последствий	**Результаты оценки риска не изменились**	Замена существующей подсистемы, притом что это не влияет на кибербезопасность результирующей архитектуры E/E, а значит, **не предполагает необходимость распространения типа**. **Это обычная ситуация**	Замена ЭБУ: • Новый современный процессор, больше памяти, никаких новых функциональных возможностей • Иной поставщик, но одни и те же технические характеристики

AJ. Пункты 9–12

«9. Соответствие производства

10. Санкции, налагаемые за несоответствие производства

11. Окончательное прекращение производства

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

Никаких руководящих указаний в отношении этого требования в настоящий документ внесено не было.

4. Руководящие указания в отношении приложения 1 к информационному документу

A. Пункты 9–9.1

«9. Кибербезопасность

9.1 Общие характеристики конструкции данного типа транспортного средства, включая:

a) системы транспортных средств, которые имеют отношение к кибербезопасности данного типа транспортного средства;

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

c) взаимодействие этих систем с другими системами данного типа транспортного средства и с внешними интерфейсами».

Примеры документов/доказательственных данных, которые могут быть предоставлены

Необходимо предусмотреть письменное описание архитектуры E/E.

B. Пункт 9.2

«9.2 Схематическое изображение типа транспортного средства»

Примеры документов/доказательственных данных, которые могут быть предоставлены

Необходимо предусмотреть схему архитектуры E/E — например, принципиальную схему.

C. Пункты 9.3–9.8

«9.3 Номер свидетельства о соответствии СОКиБ:

9.4 Документы для официального утверждения типа транспортного средства с описанием результатов оценки рисков и выявленных рисков:

9.5 Документы для официального утверждения типа транспортного средства с описанием мер по смягчению последствий, которые были реализованы на перечисленных системах, и методов, позволяющих устранить указанные риски:

9.6 Документы для официального утверждения типа транспортного средства с описанием специальных объектов для хранения и реализации программного обеспечения, услуг, приложений или данных в интересах вторичного рынка:

9.7 Документы для официального утверждения типа транспортного средства с описанием испытаний, которые были проведены для проверки кибербезопасности данного типа транспортного средства и его систем, и результатов этих испытаний:

9.8 Описание факторов, связанных с цепочкой поставок, с точки зрения кибербезопасности:»

Никаких руководящих указаний по поводу этого требования в настоящий документ внесено не было.

5. Шаблон для обмена данными через ДЕТА в соответствии с пунктом 5.3

Важное примечание:

Информация, полученная через ДЕТА для целей обмена информацией в соответствии со схемой, которая определена в Правилах ООН, должна быть защищена безопасным образом. Эта информация не должна использоваться для других целей, помимо официального утверждения типа транспортного средства и сертификации системы обеспечения кибербезопасности данного типа транспортного средства.

5.1 Описание аудиторской проверки СОКиБ

Для описания аудиторской проверки СОКиБ орган по официальному утверждению, предоставляет ДЕТА следующую информацию.

5.1.1 Процесс аудиторской проверки

Предоставляются контактные данные органа по официальному утверждению и его организационного подразделения, ответственного за проведение аудита.

Процесс аудита должен быть оформлен документально в виде технологической схемы, включающей возможные итерационные этапы и процесс устранения недостатков.

(Технологическая схема)

Хронологический рабочий процесс аудиторской проверки должен быть оформлен документально в табличной форме.

Этап аудита	*Дата начала/ временной интервал*	*Потребность в ресурсах (в человеко–днях)*
Предварительный аудит, если это необходимо, *например, привлечение аудиторов к производственным процессам, планирование аудиторских проверок, адаптация аудиторских рабочих процессов*		
Передача документов		
Подготовка к аудиторским мероприятиям, *в том числе обзор документов, например, сортировка, проверка на полноту, аудиторская проверка содержания*		
Проведение аудиторской проверки на местах		
Оценка работы по внесению исправлений, *например, исправлений, внесенных проверяемым лицом в процессе аудита проверки, может касаться выводов, сделанных в ходе аудиторской проверки*		

Этап аудита	*Дата начала/ временной интервал*	*Потребность в ресурсах (в человеко–днях)*
Подготовка и распространение отчета об аудиторской проверке		
Выводы аудиторской проверки		
Рассмотрение выводов и исправлений заявителем (в случае применимости)		
Завершение аудиторской проверки		

В случае необходимости дополнительная информация, касающаяся этапов аудиторской проверки, может быть документально оформлена в виде нижеприведенной таблицы.

Этапы аудиторской проверки	*Примечания*

Эта информация должна также включать информацию о рабочих процедурах проверки в соответствии с пунктами 6.8 и 6.10 Правил № 155 ООН и о повторной проверке в соответствии с пунктом 6.10 Правил № 155 ООН.

5.1.1.1 Проведение аудиторской проверке на местах

Если оценки СОКиБ заявителей на местах являются частью процесса аудиторской проверки, то в этом случае следует описать рабочий процесс и основные принципы (обоснование) этих оценок.

5.1.1.2 Обработка полученных данных и работа по устранение недостатков

В этой главе описывается рабочий процесс, связанный с усилиями проверяемого субъекта по устранению недостатков с учетом результатов проверки.

(Соответствующий рабочий процесс должен быть включен в блок-схему в пункте 5.1.1).

5.1.1.3 Образцы бланков заявок

Образец бланка заявки на сертификацию СОКиБ должен быть оформлен документально.

5.1.1.4 Ссылки на стандарты и спецификации

Процесс аудита и критерии оценки должны содержать ссылки на любые стандарты, спецификации или другие внешние документы (их части), которые были положены в их основу.

5.1.2 Требования к квалификации и формирование группы аудиторов

Ниже устанавливаются минимальные требования к уполномоченному органу по утверждению технических служб и аудиторов, которые проводят оценку СОКиБ. Перечень должностей в потенциальной аудиторской группе. Соответствующие уровни квалификации, которому должна соответствовать данная должность в группе аудиторов.

5.1.2.1 Возможная организация группы аудиторов

Должность *Примеры*	*Кадровые потребности* *Примеры*	*Задачи/примечания* *Примеры*
Ведущий аудитор	*1*	*Организация процесса аудита; подотчетный и ответственный*

Должность *Примеры*	*Кадровые потребности* *Примеры*	*Задачи/примечания* *Примеры*
Эксперт по процессам КБ	*2*	*Ответственный за процесс аудиторской проверки; в идеале штат кадров частично совпадает со штатом группы экспертов по официальному утверждению типа*
Эксперт по изделию	*1*	*…*
…	*…*	
Организация документооборота		

5.1.2.2 Требования к квалификации

Квалификация	*Соответствующие позиции*	*Минимальное требование*	*Подтверждение*
Уровень профессиональной подготовки	*Пример: ведущий аудитор, эксперт по процессам КБ*	*Пример: университетская степень в области информатики, математики, физики, инженерных наук или аналогичной области*	*Пример: диплом или свидетельство*
Стаж работы		*Пример: пять лет опыта работы, в том числе два года в области информационной безопасности*	*Пример: отзывы о работе*
Практический опыт			
Дополнительная подготовка			
Аккредитация			

5.1.3 Требования к аудиторской проверке

В данной главе перечислены требования к аудиторской проверке. Они должны служить доказательством, которое орган по официальному утверждению считает достаточным для подтверждения того факта, что изготовитель выполнил все требования, перечисленные в пунктах 7.2.2.1–7.2.2.5. (Включая официальные утверждения до 1 июля 2024 года).

Требования должны включать потенциальное обоснование решения о том, была ли должным образом учтена проблема кибербезопасности на этапе разработки данного типа транспортного средства.

5.1.3.1 Формальные требования

Если компетентный орган по официальному утверждению устанавливает соответствующие формальные требования, то они перечисляются здесь. Формальные требования включают, например, требования к свидетельствам, разрешениям и лицензиям.

Формальные требования	*Версия/издание, дата*
Например: сертификация по ISO 27001	

Формальные требования	*Версия/издание, дата*

5.1.3.2 Требуемая информация

В эту главу следует включить соответствующий структурированный перечень документов, которые должна представить проверяемая организация аудиторскому органу. Любые формальные требования к документации должны быть изложены здесь.

Примечание: эта информация может содержать список тем, которые необходимо рассмотреть. Возможна также ссылка на требования к документации по таким стандартным видам сертификации, как ISO/SAE 21434.

5.1.3.3 Оценка документации

В этой главе должно быть изложено детальное обоснование оценки полученной документации. В этом случае должны быть разработаны некоторые общие критерии оценки, применимые ко всей документации, например тот факт, что они находятся под контролем, используются, доступны, пересматриваются и т. д.

№	*Название*	*Описание*	*Примечания*	*Обоснование оценки*
1				Примечание: здесь должны быть указаны различные уровни обоснования. Уровень объединения процедур, связанных с требованиями и обоснованиями (с целью обеспечить их взаимное соответствие)
2				

5.1.3.4 Вопросник аудиторской проверки

<Основное направление работы 1 (*например, анализ угроз*)>

Требование	*Вопрос аудиторской проверки*	*Намерение/ цель вопроса*	*Минимальные критерии эффективности*	*Передовая практика*	*Дополнительная информация/контекст*[1]

<Основное направление работы 2 *(например, управление рисками)*>

Требование	*Вопрос аудиторской проверки*	*Намерение/ цель вопроса*	*Минимальные критерии эффективности*	*Передовая практика*	*Дополнительная информация/контекст*[1]

[1] В соответствующем случае обстоятельства, в которых данный вопрос можно задать или опустить, или возможные варианты в зависимости от контекста и т. п.

5.2 Описание официального утверждения типа

5.2.1 Процесс официального утверждения

Предоставляются контактные данные органа по официальному утверждению и его организационного подразделения, ответственного за проведение официального утверждения.

Процесс официального утверждения должен быть оформлен документально в виде соответствующей схемы работы.

(Схема работы)

5.2.2 Требования к квалификации и формирование группы экспертов

Ниже изложены минимальные требования органа по официальному утверждению к техническим службам и аудиторам, которые проводят оценку СОКиБ. Наличие перечня должностей в потенциальной группе по оценке. Каждой должности в группе должна соответствовать данная квалификация.

5.2.2.1 Возможная организация группы аудиторов

Должность Примеры	*Потребность в штатных должностях*	*Задачи/примечания*
Ведущий эксперт	*1*	*Организация процесса аудиторской проверки; подотчетный и ответственный*
Эксперт по процессам КБ	*1*	*Ответственный за передачу знаний и толкование СОКиБ в целях оценки данного типа транспортного средства; в идеале кадровый состав частично совпадает с составом группы экспертов по официальному утверждению типа*
Эксперт по изделию КБ	*2*	
Эксперт по испытанию на проникновение	*1–2*	
…		
Организация документооборота		

5.2.2.2 Требования к квалификации

Квалификация эксперта по оценке	*Соответствующие позиции*	*Минимальное требование*	*Подтверждение*
Уровень профессиональной подготовки	*Пример: ведущий эксперт по оценке, эксперт по изделию*	*Пример: университетская степень в области информатики, математики, физики, инженерных наук или аналогичной области*	*Пример: диплом или свидетельство*
Стаж работы		*Пример: пять лет опыта работы, в том числе два года в области информационной безопасности*	*Пример: отзывы о работе*
Практический опыт		*Пример: опыт работы с автомобильной сетевой архитектурой E/E и опыт работы в области оценки кибербезопасности и проверки на проникновение*	*Пример: отзывы о проекте*

Квалификация эксперта по оценке	*Соответствующие позиции*	*Минимальное требование*	*Подтверждение*
Дополнительная подготовка			
Аккредитация			

5.2.3 Требования к оценке

В настоящей главе указывается, что соответствующие меры подходят для оценки в том случае, если изготовитель транспортного средства принял необходимые меры, указанные в подпункте 5.1.1.

5.2.3.1 Общие меры безопасности

К ним относятся те меры, которые, по мнению органа по официальному утверждению, являются достаточными для проверки того факта, что:

a) данное свидетельство СОКиБ относится к данному типу транспортного средства, подлежащему официальному утверждению.

Управление рисками

b) В случае данного типа транспортного средства, подлежащего официальному утверждению, изготовитель принимает достаточные меры в целях выявления и регулирования рисков, связанных с поставщиками, включая требуемые нормы регулирования таких рисков.

Выявление рисков

c) Изготовитель транспортного средства выявляет критические элементы данного типа транспортных средств;

d) определение «критических элементов»;

e) изготовитель транспортного средства произвел исчерпывающую оценку риска для данного типа транспортного средства, как это требуется в соответствии с подпунктом 7.3.3 настоящих Правил.

Смягчение риска

f) Данный тип транспортного средства предохранен от рисков, выявленных в ходе их оценки изготовителем транспортного средства;

g) меры по смягчению последствий, применяемые изготовителем, являются соразмерными, включая разъяснение термина «соразмерные»;

h) обоснование, подтверждающее, что меры по смягчению последствий, указанные в части B или C приложения 5, неактуальны, недостаточны для выявленного риска или неосуществимы;

i) «другие меры по смягчению последствий», принимаемые изготовителем в соответствии с подпунктом 7.3.4, являются «надлежащими».

Мониторинг и реагирование

j) Принципы, заложенные в соответствующей СОКиБ в целях мониторинга угроз и реагирования на возможные инциденты, тщательно применяются на уровне данного типа транспортного средства и действуют эффективно;

k) эффективность и действенность введенных мер по смягчению последствий была проверена и находится под контролем.

Орган по официальному утверждению устанавливает на всесторонней основе соответствующие стандарты оценки, применяемые в связи с вышеупомянутой проверкой.

2.3.2 Организация документооборота

Ведется перечень необходимой документации и ожидаемого основного содержания документов. Документация пригодна для оценки требований, перечисленных в пункте 2.3.1.

2.3.3 Техническая оценка

Стратегия технической оценки излагается. Она включает предусмотренные/ применяемые испытания и стратегию проверки с целью удостовериться в том, что изготовитель транспортного средства принимает меры по обеспечению кибербезопасности, требуемые на основании правил и документально подтвержденные изготовителем. Стратегия проверки учитывает результаты тестов, выполняемых третьими сторонами. *К ним, например, относятся испытания, проведенные специализированными техническими службами или поставщиками услуг, субподрядчиками изготовителя или исследовательскими учреждениями по инициативе изготовителя или органов по официальному утверждению.*

Она также включает стратегию, используемую для тиражирования испытаний, проведенным изготовителем.

Примечание: хотя, как считается, меры по оценке, указанные в пункте 2.3.1, включают результаты оценки прошлых проверок, которые документально подтверждены изготовителем, тем не менее стратегия тиражирования предусматривает необходимость обоснования выбора соответствующей проверки, подлежащей тиражированию, равно как и способа ее тиражирования.

6. Связь с ISO/SAE DIS 21434 (E)

В нижеследующей таблице кратко излагается связь между требованиями данных Правил и соответствующими пунктами ISO/SAE DIS 21434.

Пункт	*Положения, содержащиеся в ISO/SAE DIS 21434*
7.2.1 В целях оценки орган по официальному утверждению или его техническая служба удостоверяется в том, что у изготовителя транспортного средства есть соответствующая система обеспечения кибербезопасности, и удостоверяется в ее соответствии настоящим Правилам	
Убедиться в том, что система управления кибербезопасностью установлена	*Неприменимо*
7.2.2.1 Изготовитель транспортного средства подтверждает органу по официальному утверждению или его технической службе, что их система обеспечения кибербезопасности применяется к следующим этапам: • этап разработки; • этап реализации; • этап после реализации.	
Этап разработки	Пункты 9, 10, 11, 15
Этап реализации	Пункт 12
Этап после реализации	Пункты 7, 13, 14, 15
7.2.2.2 a) процессы, используемые в организации изготовителя в целях управления системой кибербезопасности	
Общеорганизационная политика в области кибербезопасности	[RQ-05-01], [RQ-05-03]
Управление процессами, имеющими отношение к кибербезопасности	[RQ-05-02], [RQ-05-09]

Пункт	*Положения, содержащиеся в ISO/SAE DIS 21434*
a3) Формирование и поддержание культуры кибербезопасности и осведомленности	[RQ-05-07], [RQ-05-08]
7.2.2.2 b) Процессы, используемые для выявления рисков, которым подвергаются соответствующие типы транспортных средств. В рамках этих процессов рассматриваются угрозы, указанные в части A приложения 5, а также другие соответствующие угрозы	
b1) Процесс выявления рисков в области кибербезопасности для данных типов транспортных средств, установленных на этапах разработки, производства и послепродажного обслуживания	[RQ-08-01], [RQ-08-02], [RQ-08-03], [RQ-08-08], [RQ-08-09] Угрозы, указанные в приложении 5 к Правилам № 155 ООН, в сферу действия ISO/SAE 21434 не входят
7.2.2.2 c) Процессы, используемые для оценки, классификации и устранения выявленных рисков	
c1) Налажен ли процесс оценки и классификации рисков в области кибербезопасности для типов транспортных средств на этапах разработки, производства и послепродажного обслуживания?	[RQ-08-11], [RQ-08-04], [RQ-08-06], [RQ-08-10]
c2) Налажен ли процесс обработки рисков в области кибербезопасности для соответствующих типов транспортных средств на этапах разработки, производства и послепродажного обслуживания?	[RQ-08-12], [RQ-09-07], [RQ-05-06], [RQ-09-08]
7.2.2.2 d) Процессы, введенные в действие с целью удостовериться, что выявленные риски устраняются надлежащим образом	
d1) Налажен ли процесс проверки целесообразности управления рисками?	[RQ-09-09]
e) Процессы, используемые для проверки кибербезопасности соответствующего типа транспортного средства	
e1) Налажен ли процесс определения требований к кибербезопасности?	[RQ-09-10], [RQ-10-01]
e2) Налажен ли процесс валидации требований к кибербезопасности данного изделия на этапе разработки?	[RQ-11-01], [RQ-11-02]
e3) Налажен ли процесс валидации требований к кибербезопасности данного изделия на этапе производства?	[RQ-12-01]
7.2.2.2 f) Процессы, используемые с целью обеспечить постоянное обновление оценки рисков	
f1) Налажен ли процесс постоянного обновления оценки риска в области кибербезопасности?	[RQ-11-03], [RQ-06-08], [RQ-07-05], [RQ-07-06]

Пункт	*Положения, содержащиеся в ISO/SAE DIS 21434*
7.2.2.2 g) Процессы, используемые для мониторинга, обнаружения и реагирования на кибератаки, киберугрозы и факторы уязвимости соответствующих типов транспортных средств и процессов, используемых для оценки того, являются ли принимаемые меры кибербезопасности по-прежнему эффективными в свете новых киберугроз и факторов уязвимости, которые были выявлены	
g1) Налажен ли процесс мониторинга информации по кибербезопасности?	[RQ-07-01]
g2) Налажен ли процесс выявления соответствующих событий в области кибербезопасности?	[RQ-07-02]
g3) Налажен ли процесс оценки событий в области кибербезопасности и анализа факторов уязвимости в области кибербезопасности?	[RQ-07-03], [RQ-07-04]
g4) Налажен ли процесс устранения выявленных факторов уязвимости в области кибербезопасности?	[RQ-07-05], [RQ-15-04], [RQ-15-05], [RC-15-03]
g5) Налажен ли процесс реагирования на инциденты в области кибербезопасности?	[RQ-13-01], [RQ-13-02], [RQ-13-03]
g6) Налажен ли процесс валидации эффективности ответных мер?	[RQ-11-01], [RQ11-03], [RQ-11-04]
h) Процессы, используемые в целях получения соответствующих данных, необходимых для подкрепления результатов анализа предпринятых попыток проведения кибератак или успешных кибератак	
Есть ли какой-либо конкретный процесс, который позволял бы получать данные для подкрепления результатов анализа?	[RQ-07-03]
7.2.2.3 Изготовитель транспортного средства подтверждает, что процессы, используемые в его системе управления кибербезопасностью, будут обеспечивать — на основе классификации, указанной в подпунктах 7.2.2.2 c) и 7.2.2.2 g), — снижение уровня киберугроз и факторов уязвимости, которые предполагают соответствующие меры реагирования со стороны изготовителя этого транспортного средства в разумные сроки	
Смягчение последствий в разумные сроки	В ISO/SAE DIS 21434 (E) сроки не определены
7.2.2.4 Изготовитель транспортного средства подтверждает, что процессы, используемые в его системе управления кибербезопасностью, будут обеспечивать непрерывный мониторинг, указанный в подпункте 7.2.2.2 g). Они включают: a) транспортные средства после первой регистрации в системе мониторинга; b) возможности анализа и обнаружения киберугроз, факторов уязвимости и кибератак на основе данных о транспортном средстве и его сервисной книжки. Эти возможности используются с соблюдением пункта 1.3 и права владельцев или водителей автомобилей на неприкосновенность частной жизни, прежде всего в плане согласия	

Пункт	*Положения, содержащиеся в ISO/SAE DIS 21434*
Мониторинг после первой регистрации	Пункт 7.3 «Мониторинг кибербезопасности»
Возможности анализа и обнаружения киберугроз, факторов уязвимости и кибератак на основе данных о транспортном средстве и его сервисной книжки	В стандарте ISO/SAE DIS 21434 (E) прямо не упоминается, но может рассматриваться как информация по кибербезопасности
Уважение прав владельцев или водителей автомобилей на неприкосновенность частной жизни, особенно в плане согласия	В сферу действия ISO/SAE 21434 не входит, поэтому неприменимо
7.2.2.5 Изготовитель транспортного средства должен продемонстрировать, каким образом его система обеспечения кибербезопасности будет регулировать соответствующие факторы зависимости, которая может быть у него налажена с поставщиками изделий и услуг, с которыми заключены соответствующие контракты, или с его подрядными организациями, в связи с требованиями пункта 7.2.2.2	
Факторы зависимости, которые могут существовать с поставщиками, работающими на договорной основе	[RQ-06-09], [RQ-15-03], [RC-15-02]
Факторы зависимости, которые могут существовать с провайдерами услуг, работающими на договорной основе	[RQ-06-09], [RQ-15-03], [RC-15-02]
Факторы зависимости, которые могут существовать с подрядными организациями изготовителя	[RQ-06-09], [RQ-15-03], [RC-15-02]

B. Часть B

Руководящие принципы использования ДЕТА в связи с обменом информацией по вопросам кибербезопасности (в соответствии с Правилами ООН № [155])

I. Введение

1. Цель настоящего руководящего документа — сориентировать органы Договаривающихся сторон Соглашения 1958 года, которые уполномочены предоставлять официальные утверждения, относительно использования ДЕТА в процессе осуществления Правил № [155] ООН о единообразных предписаниях, касающихся официального утверждения транспортных средств в отношении кибербезопасности и системы управления кибербезопасностью (документы ECE/TRANS/WP.29/2020/79 с поправками, содержащимися в документах ECE/TRANS/WP.29/2020/94 и ECE/TRANS/WP.29/2020/97).

2. Настоящее руководство не влечет за собой изменения положений Правил ООН № 155. В случае любого несоответствия между этими руководящими принципами и текстом Правил ООН преимущественную силу имеют Правила.

3. Данный руководящий документ применяется без ущерба для любых руководств, правил и инструкций, содержащихся в справочниках, информационных пособий для пользователей, инструкций по административному сопровождению клиентов, руководящих принципов или любых иных документов ДЕТА.

4. Для целей настоящих руководящих принципов «КБ» означает «кибербезопасность», а «ДЕТА» — «База данных для обмена документацией по официальному утверждению типа, созданная Европейской экономической комиссией Организации Объединенных Наций».

II. Основные принципы обмена информацией по КБ в рамках ДЕТА

5. Пункты Правил № 155 ООН, касающиеся использования ДЕТА:

5.3.2 Каждая Договаривающаяся сторона, применяющая настоящие Правила, уведомляет и информирует через свой орган по официальному утверждению другие органы по официальному утверждению Договаривающихся сторон, применяющих настоящие Правила ООН, о методе и критериях, взятых за основу уведомляющим органом для оценки уместности мер, принятых в соответствии с настоящими Правилами, в частности с пунктами 5.1, 7.2 и 7.3.

Эта информация доводится до сведения: a) только перед первым предоставлением официального утверждения на основании настоящих Правил и b) каждый раз при обновлении метода или критериев оценки.

Эта информация предназначена для обмена в целях сбора и анализа передовой практики и обеспечения единообразного применения настоящих Правил всеми органами по официальному утверждению, применяющими настоящие Правила.

5.3.3 Информация, указанная в пункте 5.3.2, загружается на английском языке в защищенную базу данных в Интернете «ДЕТА», созданную Европейской экономической комиссией Организации Объединенных Наций, в установленные сроки и не позднее чем за 14 дней до первого предоставления официального утверждения на основании соответствующих методов и критериев оценки. Эта информация должна быть достаточной для понимания минимальных уровней эффективности, установленных органом по официальному утверждению в отношении каждого конкретного требования, указанного в пункте 5.3.2, а также процессов и мер, которые он применяет для проверки соблюдения этих минимальных уровней эффективности.

5.3.4 Органы по официальному утверждению, получающие информацию, указанную в пункте 5.3.2, могут направлять свои замечания уведомляющему органу по официальному утверждению путем их загрузки в ДЕТА в течение 14 дней после дня уведомления.

6. В разделе 5 выше изложен случай общего использования ДЕТА, когда орган по официальному утверждению предоставляет соответствующее официальное утверждение типа на основании Правил № 155 ООН (далее именуемый «уведомляющий орган»):

a) загружает требуемую информацию по КБ в ДЕТА и

b) уведомляет об этом другие органы, добавляя соответствующее уведомление в ДЕТА.

7. Информация по КБ, загружаемая в ДЕТА, доступна только для Договаривающихся сторон, применяющих Правила № 155 ООН. Уведомление будет доступно для всех пользователей ДЕТА.

III. Общие указания по использованию ДЕТА для обмена информацией по КБ

8. Уведомляющий орган действует следующим образом:

a) вся требуемая информация по КБ, упомянутая в пункте 5.3.2 Правил № 155 ООН, должна быть собрана в один или несколько файлов в формате pdf. Эти файлы загружаются как части документов типа «OTHER» («ДРУГИЕ»);

b) необходимо ввести ряд атрибутов. При этом необходимо заполнить, как минимум, обязательные поля. Это включает:

i) позиция «approval number» (номер официального утверждения), которая должна быть зарезервирована органом по официальному утверждению;

ii) позиция «approval date» (дата официального утверждения), которая является предполагаемой датой предоставления официального утверждения. Промежуток времени между этой датой и датой уведомления других органов должен составлять не менее 14 дней;

iii) позиция «approval state» (состояние официального утверждения), которая должна быть помечена «in progress» (в процессе);

c) после этого уведомляющий орган вносит фактическое уведомление в позицию «News» («Новости»). Это уведомление включает как минимум стандартный текст и номер официального утверждения для отслеживания соответствующей информации по КБ в архиве ДЕТА следующим образом:

«*Орган по официальному утверждению [название страны], настоящим уведомляет другие органы, предоставляющие официальное утверждение, Договаривающихся сторон, применяющих Правила № 155 ООН, о методе и критериях, положенных в основу оценки целесообразности мер, принятых в соответствии с Правилами № 155 ООН и, в частности, с пунктами 5.1, 7.2 и 7.3. Подробную информацию см. "type approval No [...]" ("официальное утверждение типа № [...]")*».

Примечание: «News» («Новости») не является почтовой системой. После входа в систему другие пользователи видят только сообщения. По этой причине в данных руководящих принципах органам по официальному утверждению рекомендуется ежедневно проверять раздел «News» («Новости») ДЕТА;

d) если по истечении как минимум 14 дней после сообщения об уведомлении других органов уведомляющий орган принимает решение предоставить официальное утверждение, он как можно скорее:

i) заполняет все необходимые атрибуты, включая конечный параметр в позиции «approval data» (данные официального утверждения); и

ii) загружает части документов типа «CERT», «IF» и «TR».

9. Другие органы Договаривающихся сторон, применяющих Правила № 155 ООН, которые предоставляют официальные утверждения и принимают к сведению сообщение уведомляющего органа, могут представить замечания этому органу в течение 14 дней после уведомления. В таком случае они должны:

a) отправить сообщение по электронной почте в уведомляющий орган, включая всю соответствующую информацию;

b) добавить в позицию «News» («Новости») необходимое сообщение в целях информирования других органов о том, что соответствующие замечания были переданы уведомляющему органу. Это сообщение включает, как минимум, стандартный текст и номер официального утверждения, как указано ниже:

«*Орган по официальному утверждению [название страны] настоящим информирует другие органы по официальному утверждению Договаривающихся сторон, применяющих Правила № 155 ООН, о том, что в связи с уведомлением, сделанным органом по официальному утверждению [название страны], представлены соответствующие замечания. Подробную информацию см. "type approval No [...]" ("официальное утверждение типа №...")*».

Уведомляющий орган без излишних задержек добавляет полученные замечания в архив ДЕТА, загрузив их в виде документа «OTHER» («ДРУГИЕ») в формате pdf в тот же раздел, что и первоначальные документы.

Примечание: этот порядок соблюдается с целью обеспечить доступ к информации, которая представляет собой коммерческую тайну, только тем органам Договаривающихся сторон, применяющих Правила № 155 ООН, которые предоставляют официальное утверждение.

10. Разделы 8 и 9 выше применяются до первого предоставления официального утверждения на основании Правил № 155 и каждый раз при обновлении метода или критериев оценки КБ.