Правило № 155 на ООН — Единни предписания за одобрение на превозни средства по отношение на киберсигурността и системата за управление на киберсигурността [2021/387]

Дата на влизане в сила: 22 януари 2021 г.

Настоящият документ е само средство за документиране. Автентични и правно обвързващи текстове са:

— ECE/TRANS/WP.29/2020/79

— ECE/TRANS/WP.29/2020/94 и

— ECE/TRANS/WP.29/2020/97

СЪДЪРЖАНИЕ

1. ПРИЛОЖНО ПОЛЕ

1.1. Настоящото правило се прилага по отношение на киберсигурността за превозни средства от категории M и N.

Настоящото правило се прилага също така за превозни средства от категория O, ако са оборудвани с поне един електронен блок за управление.

1.2. Настоящото правило се прилага и за превозни средства от категории L_6 и L_7, ако са оборудвани с функционални възможности за автоматизирано управление от ниво 3 нагоре, както е определено в „Справочния документ с определения за автоматизирано управление“ съгласно Работната група по член 29 и общите принципи за разработване на правила на ООН относно автоматизираните превозни средства (ECE/TRANS/WP.29/1140).

1.3. Настоящото правило не засяга други правила на ООН и регионалното или националното законодателство относно достъпа от страна на упълномощени страни до превозното средство, неговите данни, функции и ресурси, както и условията на такъв достъп. Това правило също така не засяга прилагането на националното и регионалното законодателство в областта на правото на неприкосновеност на личния живот и защитата на физическите лица във връзка с обработването на личните им данни.

1.4. Настоящото правило не засяга други правила на ООН, регионално или национално законодателство, регулиращи разработването и инсталирането/системната интеграция на резервни части и компоненти, физически и цифрови, във връзка с киберсигурността.

2. ОПРЕДЕЛЕНИЯ

За целите на настоящото правило се прилагат следните определения:

2.1. „Тип превозно средство“ означава превозни средства, които са еднакви най-малко по следните съществени характеристики:

а) Наименованието от производителя на типа превозно средство;

б) Основни аспекти на електрическата/електронната архитектура и външните интерфейси във връзка с киберсигурността.

2.2. „Киберсигурност“ означава условията, при които пътните превозни средства и техните функции са предпазени от киберзаплахи за електрическите или електронните компоненти.

2.3. „Система за управление на киберсигурността (CSMS)“ означава систематичен, основан на риска подход, определящ организационните процеси, отговорностите и управлението, с цел справяне с риска, свързан с киберзаплахите за превозните средства, и осигуряване на тяхната защита от кибератаки.

2.4. „Система“ означава набор от компоненти и/или подсистеми, които изпълняват дадена функция или функции.

2.5. „Развойна фаза“ означава периода преди одобряването на типа на даден тип превозно средство.

2.6. „Производствена фаза“ означава продължителността на производството на даден тип превозно средство.

2.7. „Следпроизводствена фаза“ означава периода, през който даден тип превозно средство вече не се произвежда до края на излизането от употреба на всички превозни средства от този тип. Превозните средства, които са свързани с конкретния тип превозно средство, продължават да се използват през тази фаза, но вече не се произвеждат. Фазата приключва, когато вече няма функциониращи превозни средства от дадения тип.

2.8. „Мярка за смекчаване“ означава мярка, която намалява риска.

2.9. „Риск“ означава вероятността при дадена заплаха да се използват уязвимостите на превозното средство, с което да се причинят вреди на организацията или на физически лица.

2.10. „Оценка на риска“ означава цялостния процес на откриване, разпознаване и описване на рисковете (установяване на рисковете) с цел да се разбере естеството на риска и да се определи нивото му (анализ на риска), както и на сравняване на резултатите от анализа на риска с критериите за риска, за да се определи дали рискът и/или размерът му е приемлив или допустим (оценка на риска).

2.11. „Управление на риска“ означава съгласувани дейности за управление и контрол на дадена организация по отношение на риска.

2.12. „Заплаха“ означава потенциална причина за нежелан инцидент, който може да доведе до вреди за дадена система, организация или физическо лице.

2.13. „Уязвимост“ означава слабост на даден актив или мярка за смекчаване, която може да бъде използвана при условия на една или повече заплахи.

3. ЗАЯВЛЕНИЕ ЗА ОДОБРЕНИЕ

3.1. Заявлението за одобрение на тип превозно средство във връзка с киберсигурността се подава от производителя на превозното средство или от негов надлежно упълномощен представител.

3.2. Към заявлението се прилагат посочените по-долу документи в три екземпляра и следните сведения:

3.2.1. Описание на типа превозно средство във връзка с елементите, посочени в приложение 1 към настоящото правило.

3.2.2. В случаите, когато се установи, че тази информация е защитена от правата за интелектуална собственост или представлява специфично технологично знание на производителя или на неговите доставчици, производителят или неговите доставчици предоставят достатъчно информация, която да позволи изчисленията да бъдат извършени правилно. Тази информация се разглежда на принципа на поверителност.

3.2.3. Сертификат за съответствие за системата за управление на киберсигурността съгласно точка 6 от настоящото правило.

3.3. Документацията се предоставя в две части:

а) Официалният комплект документи за одобрение, съдържащ материалите, посочени в приложение 1, който се предоставя на органа по одобряването или на неговата техническа служба при предаването на заявлението за одобрение на типа. Този комплект документи се използва от органа по одобряването или неговата техническа служба като основна справочна информация в процеса на одобрение. Органът по одобряването и неговата техническа служба гарантират, че този комплект документи е на разположение поне 10 години, считано от момента, в който производството на типа превозно средство се прекратява окончателно.

б) Допълнителните материали, свързани с изискванията на настоящото правило, може да бъдат задържани от производителя, но се предоставят за проверка при одобряване на типа. Производителят гарантира, че всеки материал, който е бил предоставен за проверка по време на одобряването на типа, остава наличен за период от поне 10 години, считано от момента, в който производството на типа превозно средство се прекратява окончателно.

4. МАРКИРОВКА

4.1. Върху всяко превозно средство, съответстващо на тип превозно средство, одобрен съгласно настоящото правило, на видно и леснодостъпно място, което се посочва във формуляра за одобрение, се поставя международна маркировка за одобрение, която се състои от:

4.1.1. Окръжност около буквата „E“, последвана от отличителния номер на държавата, издала одобрението.

4.1.2. Номера на настоящото правило, следван от буквата „R“, тире и номера на одобрение, отдясно на окръжността, предписана в точка 4.1.1 по-горе.

4.2. Ако превозното средство съответства на тип превозно средство, одобрен съгласно едно или няколко други правила, приложени към Спогодбата, не е необходимо да се повтаря символът, указан в точка 4.1.1 по-горе, в държавата, издала одобрението съгласно настоящото правило; в такъв случай номерата на правилото и одобрението, както и допълнителните символи за всички правила, съгласно които одобрението е било издадено в държавата, издала одобрение съгласно настоящото правило, трябва да се поставят във вертикални колони в дясно от символа, предписан в точка 4.1.1 по-горе.

4.3. Маркировката за одобрение трябва да е четлива и незаличима.

4.4. Маркировката за одобрение се поставя в близост до или на табелката с данни на превозното средство, поставена от производителя.

4.5. В приложение 3 към настоящото правило са дадени примери за оформлението на маркировката за одобрение.

5. ОДОБРЕНИЕ

5.1. Органът по одобряването предоставя, когато това е уместно, одобрение на типа във връзка с киберсигурността само за типове превозни средства, които отговарят на изискванията на настоящото правило.

5.1.1. Органът по одобряването или техническата служба потвърждават посредством проверки на документите, че производителят на превозното средства е взел необходимите мерки във връзка с типа на превозното средство с цел:

а) Да събере и потвърди информацията, която се изисква съгласно настоящото правило, по цялата верига на доставки, за да докаже, че свързаните с доставчиците рискове са определени и се управляват;

б) Да документира оценката на рисковете (изготвена по време на развойната фаза или със задна дата), резултатите от изпитванията и мерките за смекчаване, приложени за типа превозно средство, включително проектната информация, която подкрепя оценката на риска;

в) Да бъдат въведени подходящи мерки, свързани с киберсигурността, в проекта на типа превозно средство;

г) Да бъдат открити и да се реагира на евентуалните атаки срещу киберсигурността;

д) Да се води регистър на данните, за да се подпомогне откриването на кибератаки и да се осигури възможност за събиране на криминалистични данни с цел да се позволи анализ на опитите или успешните кибератаки.

5.1.2. Органът по одобряването или техническата служба потвърждават посредством изпитвания на превозното средство от съответния тип превозно средство, че производителят на превозното средства е приложил свързаните с киберсигурността мерки, които е документирал. Провеждат се изпитвания върху образци от страна на самия орган по одобряването или техническата служба или в сътрудничество с производителя на превозното средство. Изпитванията върху образци е насочено, но без да се ограничава, към рисковете, които са оценени като високи по време на оценката на рисковете.

5.1.3. Органът по одобряването или техническата служба отказват да предоставят одобрение на типа във връзка с киберсигурността, ако производителят на превозното средство не е изпълнил едно или повече от изискванията, посочени в точка 7.3, по-специално:

а) Производителят на превозното средство не е извършил изчерпателната оценка на риска, посочена в точка 7.3.3.; включително, ако производителят не е взел предвид всички рискове, свързани със заплахите, посочени в приложение 5, част А;

б) Производителят на превозното средство не е защитил типа превозно средство срещу рисковете, определени в оценката на риска от производителя на превозното средство, или не са били приложени пропорционални мерки за смекчаване, както се изисква съгласно точка 7;

в) Производителят на превозното средство не е въвел подходящи и пропорционални мерки, за да осигури специални среди за типа превозно средство (ако са предвидени) за съхранението и изпълнението на следпродажбено обслужване, включващо софтуер, услуги, приложения или данни;

г) Производителят на превозното средство не е провел преди одобряването подходящи и достатъчни изпитвания, за да потвърди ефективността на приложените мерки за сигурност.

5.1.4. Органът по одобряването, който извършва оценката, отказва да предостави одобрение на типа във връзка с киберсигурността също така, ако производителят на превозното средство не е предоставил на органа по одобряването или техническата служба достатъчна информацията, за да се оцени киберсигурността на типа превозно средство:

5.2. Страните по Спогодбата от 1958 г., които прилагат настоящото правило, биват уведомявани относно одобрението, разширяването или отказа за издаване на одобрение на тип превозно средство съгласно настоящото правило, посредством формуляр, който съответства на образеца от приложение 2 към настоящото правило.

5.3. Органът по одобряването не предоставя одобрение на типа, без да потвърди, че производителят е приложил задоволителни мерки и процедури, за да управлява по подходящ начин аспектите на киберсигурността, обхванати от настоящото правило.

5.3.1. Органът по одобряването и неговата техническа служба гарантират, в допълнение към критериите, определени в списък 2 от Спогодбата от 1958 г., че разполагат с:

а) Компетентен персонал с подходящи умения в областта на киберсигурността и конкретни знания по отношение на оценката на рисковете в автомобилния сектор ([1]);

б) Въведени процедури за еднаква оценка съгласно настоящото правило.

([1]) Напр. ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434

5.3.2. Всяка страна по Спогодбата, която прилага настоящото правило, уведомява и информира чрез своя орган по одобряването другите органи по одобряването на договарящите се страни, които прилагат настоящото правило на ООН, относно метода и критериите, които нотифициращият орган е използвал като основа, за да оцени целесъобразността на мерките, взети в съответствие с настоящото правило и по-специално с точка 5.1, 7.2 и 7.3.

Тази информация се споделя а) само преди предоставянето за първи път на одобрение съгласно настоящото правило и б) всеки път когато се актуализира методът или критериите за оценка.

Тази информация е предназначена да бъде споделяна за целите на събирането и анализа на най-добрите практики и с оглед да се гарантира последователното прилагане на настоящото правило от всички органи по одобряването, които го прилагат.

5.3.3. Информацията, посочена в точка 5.3.2, се качва на английски език в сигурната интернет база данни „DETA“ ([2]), създадена от Икономическата комисия за Европа на Организацията на обединените нации, своевременно и не по-късно от 14 дни, преди за първи път да бъде предоставено одобрение съгласно съответните методи и критерии за оценка. Информацията трябва да бъде достатъчна, за да се разбере какви минимални нива на ефективност са били приети от органа по одобряването за всяко отделно изискване, посочено в точка 5.3.2, както и процесите и мерките, които той прилага, за да потвърди съответствието с тези минимални нива на ефективност ([3]).

5.3.4. Органите по одобряването, които получават информацията, посочена в точка 5.3.2, може да представят на нотифициращия орган по одобряването коментари, като ги качат в DETA в рамките на 14 дни след деня на известието.

5.3.5. Ако не е възможно издаващият одобрението орган да вземе предвид коментарите, получени в съответствие с точка 5.3.4, органите по одобряването, които са изпратили коментарите, и издаващият одобрението орган трябва да потърсят допълнителни пояснения в съответствие със списък 6 от Спогодбата от 1958 г. Съответната помощна работна група ([4]) към Световния форум за хармонизация на регулаторната уредба за превозните средства (WP.29) за това правило се договаря относно общо тълкуване на методите и критериите за оценка ([5]). Това общо тълкуване се прилага и всички органи по одобряването съответно издават одобрения на типа съгласно настоящото правило.

5.3.6. Всеки орган по одобряването, който предоставя одобрение на типа съгласно настоящото правило, известява другите органи по одобряването относно предоставеното одобрение. В рамките на 14 дни след предоставянето на одобрението органът по одобряването качва в DETA на английски език одобрението на типа, заедно с допълнителната документация ([6]).

5.3.7. Договарящите се страни може да разгледат предоставените одобрения на основата на информацията, качена съгласно точка 5.3.6. В случай на различие в мненията между договарящите се страни, това се разрешава в съответствие с член 10 и списък 6 от Спогодбата от 1958 г. Договарящите се страни също така информират съответната помощна работна група към Световния форум за хармонизация на регулаторната уредба за превозните средства (WP.29) относно различаващите се тълкувания по смисъла на списък 6 от Спогодбата от 1958 г. Съответната работна група съдейства за разрешаването на различията в мненията и може да се консултира с WP.29 относно това, ако е необходимо.

5.4. За целите на точка 7.2 от настоящото правило производителят гарантира, че се прилагат аспектите, свързани със киберсигурността, обхванати в настоящото правило.

([2]) https://www.unece.org/trans/main/wp29/datasharing.html

([3]) Насоки относно подробната информация (напр. метод, критерии, ниво на ефективност), която трябва да бъде качена, и нейния формат се предоставят в тълкувателния документ, който понастоящем се изготвя от оперативната група по киберсигурността и безжичните комуникации за седмото заседание на GRVA.

([4]) Работна група по автоматизираните/автономните и свързаните превозни средства (GRVA)

([5]) Това тълкуване се отразява в тълкувателния документ, посочен в бележката под линия към точка 5.3.3.

([6]) Допълнителна информация относно минималните изисквания за комплекта документи ще бъде изготвена от GRVA по време на седмото ѝ заседание.

6. СЕРТИФИКАТ ЗА СЪОТВЕТСТВИЕ ЗА СИСТЕМА ЗА УПРАВЛЕНИЕ НА КИБЕРСИГУРНОСТТА

6.1. Договарящите се страни определят орган по одобряването, който да извърши оценката на производителя и да издаде сертификат за съответствие за системата за управление на киберсигурността.

6.2. Производителят на превозното средство или неговият надлежно упълномощен представител подава заявление за сертификат за съответствие за системата за управление на киберсигурността.

6.3. То се придружава от посочените по-долу документи в три екземпляра и от следните данни:

6.3.1. Документи, в които е описана системата за управление на киберсигурността.

6.3.2. Подписана декларация въз основа на образеца, определен в допълнение 1 към приложение 1.

6.4. В контекста на оценката производителят декларира, че използва образеца, определен в допълнение 1 към приложение 1, и доказва по задоволителен за органа по одобряването или неговата техническа служба начин, че разполага с необходимите процедури, за да спази всички изисквания по отношение на киберсигурността съгласно настоящото правило.

6.5. Когато тази оценка е била завършена по задоволителен начин и при получаване на подписана декларация на производителя съгласно образеца, определен в допълнение 1 към приложение 1, на производителя се предоставя сертификат, озаглавен Сертификат за съответствие за система за управление на киберсигурността, както е определен в приложение 4 към настоящото правило (наричан по-долу „сертификата за съответствие за система за управление на киберсигурността“).

6.6. Органът по одобряването или неговата техническа служба използват образеца, определен в приложение 4 към настоящото правило, за сертификата за съответствие за система за управление на киберсигурността.

6.7. Сертификатът за съответствие за система за управление на киберсигурността остава валиден за максимален срок от три години, считано от датата на връчване на сертификата, освен ако той не бъде оттеглен.

6.8. Органът по одобряването, който е предоставил сертификата за съответствие за система за управление на киберсигурността, може по всяко време да провери дали изискванията за него продължават да бъдат спазвани. Органът по одобряването отнема сертификата за съответствие за система за управление на киберсигурността, ако определените в настоящото правило изисквания вече не са изпълнени.

6.9. Производителят информира органа по одобряването или неговата техническа служба относно всички промени, които засягат обстоятелствата, въз основа на които е бил издаден сертификата за съответствие за система за управление на киберсигурността. След консултация с производителя органът по одобряването или неговата техническа служба решават дали са необходими нови проверки.

6.10. В своевременен срок, позволяващ на органа по одобряването да завърши своята оценка преди края на срока на валидност на сертификата за съответствие за система за управление на киберсигурността, производителят подава заявление за нов сертификат или за удължаване на срока на валидност на съществуващия сертификат за съответствие за система за управление на киберсигурността. В случай на положителна оценка органът по одобряването издава нов сертификат за съответствие за система за управление на киберсигурността или удължава неговия срок на валидност за допълнителен срок от три години. Органът по одобряването потвърждава, че сертификатът за съответствие за система за управление на киберсигурността продължава да отговаря на изискванията на настоящото правило. Органът по одобряването издава нов сертификат в случаи, при които органът по одобряването или неговата техническа служба са били уведомени относно промени и тези промени са получили положителна повторна оценка.

6.11. Изтичането на срока или отнемането на сертификата за съответствие за система за управление на киберсигурността на производителя се счита, по отношение на типовете превозно средство, за които се отнася съответната система за управление на киберсигурността, като изменение на одобрението, както е посочено в точка 8, което може да включва отнемане на одобрението, ако условията за предоставянето на одобрението вече не са спазени.

7. СПЕЦИФИКАЦИИ

7.1. Общи спецификации

7.1.1. Изискванията на настоящото правило не ограничават разпоредбите или изискванията на други правила на ООН.

7.2. Изисквания за системата за управление на киберсигурността

7.2.1. За целите на оценката органът по одобряването или неговата техническа служба потвърждават, че производителят на превозното средства разполага с внедрена система за управление на киберсигурността, и проверяват нейното съответствие с настоящото правило.

7.2.2. Системата за управление на киберсигурността обхваща следните аспекти:

7.2.2.1. Производителят на превозното средство доказва пред органа по одобряването или техническата служба, че системата за управление на киберсигурността се прилага за следните фази:

а) Развойна фаза;

б) Производствена фаза;

в) Следпроизводствена фаза:

7.2.2.2. Производителят на превозното средство доказва, че процедурите, използвани в неговата система за управление на киберсигурността, гарантират, че се обръща достатъчно внимание на сигурността, включително на рисковете и мерките за смекчаване, изброени в приложение 5. Това включва:

а) Процедурите, използвани в организацията на производителя, за да се управлява киберсигурността;

б) Процедурите, използвани, за да се определят рисковете за типовете превозни средства. В рамките на тези процедури се вземат предвид заплахите, посочени в приложение 5, част А, и съответните други заплахи;

в) Процедурите, използвани за оценка, категоризация и третиране на откритите рискове;

г) Процедурите, които са въведени, за да се потвърди, че откритите рискове се управляват по подходящ начин;

д) Процедурите, използвани за изпитване на киберсигурността на даден тип превозно средство.

е) Процедурите, използвани, за да се гарантира, че оценката на риска остава актуална;

ж) Процедурите, използвани, за да се следят, откриват и да се реагира на кибератаките, киберзаплахите и уязвимостите, свързани с типовете превозни средства, и процесите, които се използват, за да се оцени дали въведените мерки за киберсигурност все още са ефективни с оглед на новите киберзаплахи и уязвимости, които са били открити.

з) Процедурите, използвани за осигуряването на надеждни данни, за да се подкрепят анализите на опитите или успешните кибератаки.

7.2.2.3. Производителят на превозното средство доказва, че процедурите, използвани в рамките на неговата система за управление на киберсигурността, гарантират, че въз основа на категоризацията, посочена в точка 7.2.2.2, буква в) и точка 7.2.2.2, буква ж) киберзаплахите и уязвимостите, които изискват реакция от страна на производителя на превозното средство, се смекчават в разумен срок.

7.2.2.4. Производителят на превозното средство доказва, че процесите, използвани в неговата система за управление на киберсигурността, гарантират, че мониторингът, посочен в точка 7.2.2.2, буква ж), е непрекъснат. Това включва:

а) Превозни средства след първата им регистрация в мониторинга;

б) Възможността да се анализират и откриват киберзаплахи, уязвимости и кибератаки с помощта на данните и регистрите на превозното средство. В рамките на тази възможност се спазва точка 1.3 и правото на неприкосновеност на личния живот на собствениците или шофьорите на автомобили, по-специално по отношение на съгласието.

7.2.2.5. От производителя на превозното средство се изисква да демонстрира как неговата система за управление на киберсигурността ще управлява зависимостите, които може да съществуват с доставчици, с които е сключил договор,, доставчици на услуги или подразделения на организацията на производителя по отношение на изискванията на точка 7.2.2.2.

7.3. Изисквания за типове превозни средства

7.3.1. Производителят на превозното средство трябва да разполага с валиден сертификат за съответствие за системата за управление на киберсигурността, приложима за типа превозно средство, който е обект на одобряването.

Въпреки това за одобрения на типа преди 1 юли 2024 г., ако производителят на превозното средство може да докаже, че не е възможно типът превозно средство да бъде разработен в съответствие със системата за управление на киберсигурността, тогава производителят на превозното средство трябва да докаже, че киберсигурността е била взета предвид в достатъчна степен по време на развойната фаза на съответния тип превозно средство.

7.3.2. Производителят на превозното средство открива и управлява свързаните с доставчици рискове за типа превозно средство, обект на одобрението.

7.3.3. Производителят на превозното средство определя елементите от критично значение на типа превозно средство, изготвя изчерпателна оценка на риска за типа превозно средство и третира/управлява откритите рискове по подходящ начин. В оценката на риска се вземат предвид отделните елементи на типа превозно средство и тяхното взаимодействие. Също така в оценката на риска се вземат предвид взаимодействията с всички външни системи. При оценката на риска производителят на превозното средство обръща внимание на рисковете, свързани с всички заплахи, посочени в приложение 5, част А, както и всички други съответни рискове.

7.3.4. Производителят на превозното средство защитава типа превозно средство срещу рисковете, определени в оценката на риска от производителя на превозното средство. За да бъде защитен типът превозно средство, се прилагат пропорционални мерки за смекчаване. Приложените мерки за смекчаване включват всички мерки за смекчаване, посочени в приложение 5, части Б и В, които са приложими за откритите рискове. Ако обаче дадена мярка за смекчаване, посочена в приложение 5, част Б или В, не е приложима или не е достатъчна за открития риск, производителят на превозното средство гарантира, че се прилага друга подходяща мярка за смекчаване.

По-специално, за одобрения на типа преди 1 юли 2024 г. производителят на превозното средство гарантира, че е приложена друга подходяща мярка за смекчаване, ако дадена мярка за смекчаване, посочена в приложение 5, части Б или В, е технически неприложима. Производителят представя на органа по одобряването съответната оценка на техническата приложимост.

7.3.5. Производителят на превозното средство въвежда подходящи и пропорционални мерки, за да осигури специални среди за типа превозно средство (ако са предвидени) за съхранението и изпълнението на следпродажбено обслужване, включващо софтуер, услуги, приложения или данни.

7.3.6. Производителят на превозното средство провежда преди одобряването подходящи и достатъчни изпитвания, за да потвърди ефективността на приложените мерки за сигурност.

7.3.7. Производителят на превозното средство въвежда мерки за типа превозно средство с цел:

а) да се откриват и предотвратяват кибератаките срещу превозните средства от този тип;

б) да се подкрепя способността на производителя на превозното средство за наблюдение по отношение на откриването на заплахи, уязвимости и кибератаки, свързани с типа превозно средство;

в) да се осигури възможност за събиране на криминалистични данни, за да се позволи анализ на опитите или успешните кибератаки.

7.3.8. Това определение ще се използва изключително за целите на настоящото правило. Ако използваните криптографски модули не съответстват на стандартите, по отношение на които е постигнат консенсус, производителят на превозното средство трябва да обоснове тяхното използване.

7.4. Разпоредби за докладване

7.4.1. Производителят на превозното средство докладва на органа по одобряването или техническата служба най-малко веднъж годишно или по-често, ако е приложимо, резултата от действията по наблюдението, както са определени в точка 7.2.2.2, буква ж), което трябва да включва съответната информация относно новите кибератаки. Производителят на превозното средство също така докладва и потвърждава пред органа по одобряването или техническата служба, че мерките за смекчаване във връзка с киберсигурността, приложени за неговите типове превозни средства, все още са ефективни, като уведомява и за всички допълнителни предприети действия.

7.4.2. Органът по одобряването или техническата служба проверява предоставената информация и, ако е необходимо, изисква от производителя на превозното средство да предприеме коригиращи действия относно всички открити неефективности.

Ако докладването или отговорът не са достатъчни, органът по одобряването може да реши да отнеме сертификата за съответствие за системата за управление на киберсигурността в съответствие с точка 6.8.

8. ИЗМЕНЕНИЯ НА ТИП ПРЕВОЗНО СРЕДСТВО И РАЗШИРЯВАНЕ НА ОДОБРЕНИЕТО НА ТИПА

8.1. Органът по одобряването, който е одобрил дадения тип превозно средство, трябва да бъде известен относно всяко изменение на типа превозно средство, което влияе на неговите технически характеристики по отношение на киберсигурността и/или документацията, изисквана съгласно настоящото правило. В такъв случай органът по одобряването може:

8.1.1. Да прецени, че направените изменения все още отговарят на изискванията и документацията за съществуващото одобрение на типа; или

8.1.2. Да извърши необходимата допълнителна оценка съгласно точка 5 и да изиска, ако това е необходимо, допълнителен доклад за изпитвания от техническата служба, която отговаря за провеждането на изпитвания.

8.1.3. Уведомяването относно потвърждението или разширяването или отказа за предоставяне на одобрение, в които се посочват измененията, се извършва посредством формуляр за съобщение, който съответства на образеца от приложение 2 към настоящото правило. Органът по одобряването, който издава разширение на одобрението, присвоява сериен номер на това разширение и уведомява за това останалите страни по Споразумението от 1958 г., които прилагат настоящото правило, чрез формуляр за съобщение, отговарящ на образеца от приложение 2 към настоящото правило.

9. СЪОТВЕТСТВИЕ НА ПРОИЗВОДСТВОТО

9.1. Процедурите за съответствие на производството трябва да съответстват на указаните в Споразумението от 1958 г., приложение 1 (E/ECE/TRANS/505/Rev.3), при следните изисквания:

9.1.1. Титулярят на одобрението осигурява регистриране на резултатите от изпитванията за проверка на съответствието на производството и достъп до приложените документи в продължение на определен период, съгласуван с органа по одобряването или неговата техническата служба. Този период не трябва да бъде по-дълъг от 10 години от момента на окончателното прекратяване на производството.

9.1.2. Органът по одобряването, издал одобрението на типа, може по всяко време да проверява методите за контрол на съответствието, прилагани във всяко производствено предприятие. Нормалната честота на тези проверки е веднъж на три години.

10. САНКЦИИ ПРИ НЕСЪОТВЕТСТВИЕ НА ПРОИЗВОДСТВОТО

10.1. Одобрението, издадено по отношение на тип превозно средство съгласно настоящото правило, може да бъде отнето, ако не е спазено изискването, определено в настоящото правило, или образци на превозното средство не съответстват на изискванията от настоящото правило.

10.2. Ако даден орган по одобряването отнеме одобрение, което е издал, той трябва незабавно да уведоми за това договарящите се страни, прилагащи настоящото правило, чрез формуляр за съобщение по образеца от приложение 2 към настоящото правило.

11. ОКОНЧАТЕЛНО ПРЕКРАТЯВАНЕ НА ПРОИЗВОДСТВО

11.1. Ако притежателят на одобрение прекрати окончателно производството на типа превозно средство, одобрено съгласно настоящото правило, той трябва да уведоми за това органа, издал одобрението. При получаването на съответното съобщение този орган на свой ред уведомява за това останалите страни по Спогодбата, прилагащи настоящото правило, посредством копие на формуляра за одобрение, съдържащо най-долу следните думи, изписани с едър шрифт, подписано и с поставена дата: „ПРЕКРАТЕНО ПРОИЗВОДСТВО“.

12. НАИМЕНОВАНИЯ И АДРЕСИ НА ТЕХНИЧЕСКИТЕ СЛУЖБИ, ОТГОВАРЯЩИ ЗА ПРОВЕЖДАНЕТО НА ИЗПИТВАНИЯ ЗА ОДОБРЯВАНЕ, КАКТО И НА ОРГАНИТЕ ПО ОДОБРЯВАНЕТО НА ТИПА

12.1. Страните по Спогодбата, прилагащи настоящото правило, съобщават на секретариата на ООН наименованията и адресите на техническите служби, отговарящи за провеждане на изпитванията за одобрение, както и на органите по одобряването на типа, издаващи одобрение, и на които се изпращат формулярите, удостоверяващи одобрение, разширение, отказ или отнемане на одобрение, издадени в други държави.

ПРИЛОЖЕНИЕ 1

Списък с данни

Следната информация, ако е приложима, трябва да бъде предоставяна в три екземпляра и да включва съдържание. Всички чертежи се представят в подходящ мащаб и достатъчно подробно във формат A4 или в папка с формат A4. Снимките, когато има такива, трябва да са достатъчно подробни.

1. Марка (търговско наименование на производителя): .....

2. Тип и общо търговско описание/я: .....

3. Начини за идентификация на типа, когато той е обозначен върху превозното средство: .....

4. Местоположение на маркировката: .....

5. Категории превозни средства: .....

6. Наименование и адрес на производителя/представителя на производителя: .....

7. Наименование(я) и адрес(и) на предприятието(ята) за сглобяване: .....

8. Снимка/снимки и/или чертеж/чертежи на представително превозно средство: .....

9. Киберсигурност

9.1. Общи конструктивни характеристики на типа превозно средство, включително:

а) Системи на превозното средство, които са свързани с киберсигурността на типа превозно средство;

б) Компоненти на системите, които са свързани с киберсигурността;

в) Взаимодействия на тези системи с други системи в рамките на типа превозно средство и с външни интерфейси.

9.2. Схематично представяне на типа превозно средство

9.3. Брой на сертификатите за съответствие за системата за управление на киберсигурността: .....

9.4. Документи за типа превозно средство, подлежащ на одобряване, в които са описани резултатите от неговата оценка на риска и установените рискове: .....

9.5. Документи за типа превозно средство, подлежащ на одобряване, в които са описани мерките за смекчаване, приложени за изброените системи или за типа превозно средство, и как те влияят на посочените рискове: .....

9.6. Документи за типа превозно средство, подлежащ на одобряване, в които е описана защитата на специалните среди за следпродажбено обслужване във връзка със софтуер, услуги, приложения или данни. .....

9.7. Документи за типа превозно средство, подлежащ на одобряване, в които е описано какви изпитвания са били използвани, за да се потвърди киберсигурността на типа превозно средство и неговите системи, и резултатите от тези изпитвания: .....

9.8. Описание на съображенията относно веригата на доставки във връзка с киберсигурността: .....

Допълнение 1 към приложение 1

Образец на декларация на производителя за съответствие за системата за управление на киберсигурността

Декларация на производителя за съответствие с изискванията за системата за управление на киберсигурността.

Наименование на производителя: .....

Адрес на производителя: .....

..... (*наименование на производителя*) декларира, че необходимите процеси за осигуряване на съответствие с изискванията за системата за управление на киберсигурността, определени в точка 7.2 от Правило № 155 на ООН, са инсталирани и ще се поддържат..... ....

Съставено във: ..... (*място*)

Дата: .....

Име на подписващото лице: .....

Длъжност на подписващото лице: .....

.....

(*Име и подпис на представителя на производителя*)

ПРИЛОЖЕНИЕ 2

Съобщение

(Максимален формат: A4 (210 x 297 mm)

издадено от: Наименование на администрацията:
.....
.....
.....

Относно (2) Издадено одобрение
Разширяване на одобрение
Отнемане на одобрение, считано от дд/мм/гггг
Отказ на одобрение
Окончателно прекратяване на производство

на тип превозно средство съгласно Правило № 155 на ООН

Одобрение №: .....

Разширение №: .....

Основание за разширението: .....

1. Марка (търговско наименование на производителя): .....

2. Тип и общо търговско описание(я) .....

3. Начини за идентификация на типа, когато той е обозначен върху превозното средство: .....

3.1. Местоположение на маркировката: .....

4. Категории превозни средства: .....

5. Наименование и адрес на производителя/представителя на производителя: .....

6. Наименование(я) и адрес(и) на производствения(те) завод(и): .....

7. Брой на сертификатите за съответствие за система за управление на киберсигурността: .....

8. Техническа служба, отговаряща за провеждане на изпитванията: .....

9. Дата на протокола от изпитването: .....

10. Номер на протокола от изпитването: .....

11. Забележки: (ако има такива). .....

12. Място: .....

13. Дата: .....

14. Подпис: .....

15. Прилага се индексът на информационния пакет, депозиран при органа по одобряването, който може да бъде получен при поискване:

([1]) Отличителен номер на държавата, която е предоставила/разширила/отказала/отнела одобрение (вж. разпоредбите относно одобрението в правилото)

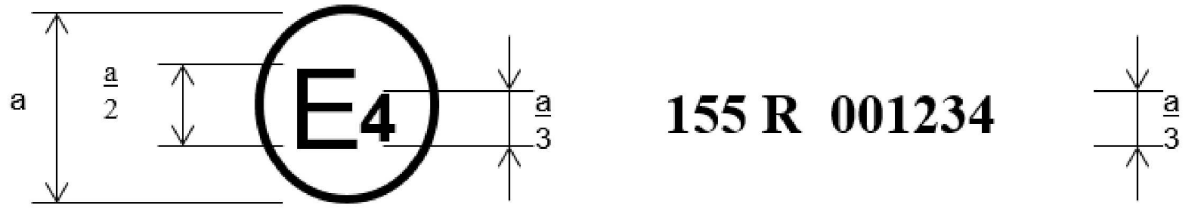
([2]) Зачеркнете неприложимото.:

ПРИЛОЖЕНИЕ 3

Разположение на знака за одобрение

ОБРАЗЕЦ А

(виж точка 4.2 от настоящото правило)



a = 8 mm (минимум)

Горепоказаната маркировка за одобрение, поставена на превозно средство, показва, че съответният тип пътно превозно средство е одобрен в Нидерландия (E 4) съгласно Правило № 155 с одобрение № 001234. Двете първи цифри на номера на одобрението показват, че то е предоставено в съответствие с изискванията на настоящото правило в първоначалната му версия (00).

ПРИЛОЖЕНИЕ 4

Образец на сертификат за съответствие за система за управление на киберсигурността

Сертификат за съответствие за система за управление на киберсигурността

с Правило № 155 на ООН

Номер на сертификата [*Номер*]

[……. *Орган по одобряването*]

Удостоверява, че

Производител: ……

Адрес на производителя: ……

в съответствие с разпоредбите на точка 7.2 от Правило № 155

Извършени са проверки на: ……

от страна на (име и адрес на органа по одобряването или техническата служба): ……

Номер на протокола: ……

Сертификатът е валиден до […… *дата*]

Съставено в […… *място*]

На … [……*дата*]

[……*подпис*]

Приложения: описание от производителя на системата за управление на киберсигурността.

ПРИЛОЖЕНИЕ 5

Списък на заплахите и съответните мерки за смекчаване

1. Настоящото приложение се състои от три части: В част А от настоящото приложение е описано базовото равнище за заплахите, уязвимостите и методите за компютърни атаки. В част Б от настоящото приложение са описани мерките за смекчаване на заплахите, които са насочени към типовете превозни средства. В част В са описани мерките за смекчаване на заплахите, които са насочени към областите извън превозните средства, напр. изчислителните машини с базите данни.

2. Част А, част Б и част В се вземат предвид с оглед на оценката на риска и мерките за смекчаване, които се прилагат от производителите на превозни средства.

3. Уязвимостите на високо равнище и съответните примери за тях са индексирани в част А. Същото индексиране е използвано в таблиците в части Б и В, за да бъдат свързани всички атаки/уязвимости със списък на съответните мерки за смекчаване.

4. В анализа на заплахите се вземат предвид и възможните въздействия от атаките. Това може да помогне да се определи сериозността на риска и да бъдат установени допълнителни рискове. Възможните въздействие от атаките може да включват:

   а) Безопасната експлоатация на превозното средство е засегната.

   б) Функции на превозното средство спират да работят;

   в) Изменения на софтуера, промяна в показателите;

   г) Софтуерът е изменен, но няма въздействие върху работата;

   д) Нарушение на целостта (валидността) на данните;

   е) Нарушение на поверителността на данните;

   ж) Загуба на наличността на данните;

   з) Други, включително престъпления.

Част А. Уязвимост или метод на атака, свързани със заплахите

1. Описания на високо равнище на заплахите и съответните уязвимости или методи на атака са изброени в таблица А1.

Таблица А1

Списък на уязвимостите или методите на атака, свързани със заплахите

Описание на високо равнище и подравнища на уязвимостите/заплахите			Пример за уязвимост или метод на атака	
4.3.1. Заплахи, свързани със сървъри за данни и функционална логика, по отношение на превозни средства в експлоатация	1	Сървъри за данни и функционална логика, използвани като средство за атакуване на превозно средство или за извличане на данни	1.1	Злоупотреби с привилегии от страна на персонала (атака от вътрешно лице)
			1.2	Неупълномощен достъп чрез интернет до сървъра (което е било възможно например посредством „задни вратички“, некоригирани уязвимости на системния софтуер, атаки SQL или други средства)
			1.3	Неупълномощен физически достъп до сървъра (извършен например чрез памет USB или друг носител, свързан към сървъра)
	2	Услугите от сървъра за данни и функционална логика са нарушени, което въздейства на функционирането на превозното средство	2.1	Атака срещу сървъра за данни и функционална логика прекратява неговото функциониране — например възпрепятства го да взаимодейства с превозни средства и да предоставя услуги, които са им необходими

Описание на високо равнище и подравнища на уязвимостите/заплахите			Пример за уязвимост или метод на атака	
	3	Данни, свързани с превозното средство и съхранявани на сървъри за данни и функционална логика, са загубени или компрометирани („нарушение на сигурността на данните“)	3.1	Злоупотреби с привилегии от страна на персонала (атака от вътрешно лице)
			3.2	Загуба на информация в изчислителния облак. Когато данните се съхраняват от доставчици на компютърни услуги „в облак“ трети страни, чувствителни данни може да бъдат загубени поради атаки или инциденти
			3.3	Неупълномощен достъп чрез интернет до сървъра (което е било възможно например посредством задни вратички, некоригирани уязвимости на системния софтуер, атаки SQL или други средства)
			3.4	Неупълномощен физически достъп до сървъра (извършен например чрез памет USB или друг носител, свързан към сървъра)
			3.5	Нарушение на сигурността на информацията поради неумишлено споделяне на данни (напр. грешки на администратор)
4.3.2. Заплахи за превозните средства по отношение на техните комуникационни канали	4	Фалшифициране на съобщения или данни, получавани от превозното средство	4.1	Фалшифициране на съобщения чрез измама на основата на прилика (напр. 802.11p V2X по време на групиране на превозни средства, съобщения от ГНСС и т.н.)
			4.2	Атака Sybil (с цел да бъдат имитирани други превозни средства, за да се създаде впечатление, че на пътя има много превозни средства)
	5	Комуникационните канали се използват за извършването на неупълномощена манипулация, изтриване или други изменения на кода/данните, които се съхраняват в превозното средство	5.1	Комуникационните канали позволяват инжектирането на код, например подправени двоични софтуерни данни може да бъдат инжектирани в комуникационния поток
			5.2	Комуникационните канали позволяват манипулиране на данни/код, съхранявани на превозното средство
			5.3	Комуникационните канали позволяват презаписване на данни/код, съхранявани на превозното средство
			5.4	Комуникационните канали позволяват изтриване на данни/код, съхранявани на превозното средство
			5.5	Комуникационните канали позволяват въвеждането на данни/код в превозното средство (запис на код от данни)
	6	Комуникационните канали позволяват да бъдат приети ненадеждни съобщения или са уязвими към отвличане на сесията/атаки с повторно възпроизвеждане	6.1	Приемане на информация от ненадежден източник
			6.2	Атака тип „посредник“/отвличане на сесията
			6.3	Атака с повторно възпроизвеждане — например атака срещу комуникационен шлюз позволява на атакуващият да върне по-старата версия на софтуера на електронен блок за управление или на софтуера на производителя на шлюза

Описание на високо равнище и подравнища на уязвимостите/заплахите			Пример за уязвимост или метод на атака	
	7	Информацията може лесно да бъде оповестена. Например чрез подслушване на комуникациите или чрез позволяване на неупълномощен достъп до чувствителни файлове или папки	7.1	Прихващане на информация / смущаващи електромагнитни излъчвания / следене на комуникациите
			7.2	Получаване на неупълномощен достъп до файлове или данни
	8	Атаки за отказ на услуга чрез комуникационните канали с цел да бъдат възпрепятствани функциите на превозното средство	8.1	Изпращане на голям брой ненужни данни към информационната система на превозното средство, така че да не може да предоставя услуги както при нормални условия
			8.2	Атака тип „черна дупка“ — с цел да бъде нарушена комуникацията между превозните средства, атакуващият успява да блокира съобщенията между превозните средства
	9	Потребител без привилегии успява да получи привилегирован достъп до системите на превозното средство	9.1	Потребител без привилегии успява да получи привилегирован достъп, например достъп до кореновата файлова система
	10	Вируси, вградени в комуникационно устройство, може да инфектират системите на превозното средство	10.1	Вирус, вграден в комуникационно устройство, инфектира системите на превозното средство
	11	Съобщения, получени от превозното средство (например X2V или съобщения за диагностика) или предавани в рамките на системите му, съдържат зловредно съдържание	11.1	Зловредни вътрешни (напр. от протокола CAN) съобщения
			11.2	Зловредни V2X съобщения, напр. инфраструктура към превозното средство или съобщения между превозни средства (напр. протоколи CAM, DENM)
			11.3	Зловредни съобщения за диагностика
			11.4	Зловредни съобщения, обект на интелектуална собственост (напр. обичайно изпращаните от производител на оригинално оборудване или доставчик на компонент/система/функция)
4.3.3. Заплахи за превозните средства по отношение на техните процедури за актуализиране	12	Злоупотреба или компрометиране на процедури за актуализиране	12.1	Компрометиране на предавани по ефира процедури за актуализиране на софтуера. Това включва фалшифициране на програмата или софтуера на производителя за актуализиране на системата
			12.2	Компрометиране на локални/физически процедури за актуализиране на софтуера. Това включва фалшифициране на програмата или софтуера на производителя за актуализиране на системата
			12.3	Софтуерът се подправя преди процеса на актуализиране (и следователно е повреден), макар че процесът на актуализиране не е засегнат

Описание на високо равнище и подравнища на уязвимостите/заплахите			Пример за уязвимост или метод на атака	
			12.4	Компрометиране на криптографски ключове на доставчика на софтуер, за да се осигури възможност за невалидно актуализиране
	13	Възможно е да бъдат възпрепятствани официални актуализации	13.1	Атака тип „отказ на услуга“ срещу сървър или мрежа за актуализиране с цел да се възпрепятства внедряването на актуализации на софтуера от критично значение и/или отключването на специфични за потребителя функции
4.3.4. Заплахи за превозни средства, свързани с неумишлени човешки действия, които улесняват извършването на кибератака	15	Легитимни участници може да предприемат действия, с които несъзнателно да улеснят извършването на кибератака	15.1	Невинна жертва (напр. собственик, оператор или инженер по поддръжката) е измамена да предприеме действие, така че непреднамерено да зареди зловреден софтуер или да осигури възможност за атака
			15.2	Определените процедури за сигурност не се спазват
4.3.5. Заплахи за превозните средства, свързани с техните външни връзки	16	Манипулиране на връзките на функциите на превозното средство осигурява възможност за кибератака — това може да включва телематика, системи, които позволяват операции от разстояние, и системи, които използват безжични връзки с малък обсег	16.1	Манипулиране на функции, предназначени за дистанционно управление на системи, като например ключове, имобилайзери и колони за зареждане
			16.2	Манипулиране на телематиката на превозното средство (напр. манипулиране на измерването на температурата на чувствителни стоки, дистанционно отключване на товарните врати)
			16.3	Смущаване на безжични връзки или датчици с малък обсег
	17	Софтуер на трета страна, ползващ хостинг, напр. развлекателни приложения, използвани като средство, за да се атакуват системите на превозното средство	17.1	Компрометирани приложения или приложения с ниско ниво на сигурност на софтуера, използвани като метод за атакуване на системите на превозното средство
	18	Устройства, свързани с външни интерфейси, напр. портове USB, порт OBD, използвани като средство за атакуване на системите на превозното средство	18.1	Външни интерфейси като например USB или други портове, използвани като точка на атака — например чрез инжектиране на код
			18.2	Носител, който е заразен с вирус, е свързан със система на превозното средство
			18.3	Достъп за диагностика (напр. хардуерен ключ в порт OBD), използван за осигуряване на възможност за атака, напр. манипулиране на параметрите на превозното средство (пряко или непряко)
4.3.6. Заплахи за данните/кода на превозното средство	19	Извличане на данни/код на превозното средство	19.1	Извличане на защитен от авторско право или лицензиран софтуер от системите на превозното средство (пиратиране на продукт)
			19.2	Неупълномощен достъп до поверителна информация на собственика, като например самоличност, информация за платежна сметка, информация от адресния указател, информация относно местоположението, електронен идентификатор на превозното средство и т.н.
			19.3	Извличане на криптографски ключове

Описание на високо равнище и подравнища на уязвимостите/заплахите			Пример за уязвимост или метод на атака	
	20	Манипулиране на данни/код на превозното средство	20.1	Незаконни/неупълномощени промени на електронния идентификатор на превозното средство
			20.2	Използване на фалшива самоличност. Например, ако даден потребител иска да покаже друга самоличност, когато осъществява комуникация със системите за пътна такса, сървъра за данни и функционална логика на производителя
			20.3	Действия за заобикаляне на системите за следене (напр. хакерство/ подправяне/ блокиране на съобщения, като например данни от ODR Tracker, или брой изпълнения)
			20.4	Манипулиране на данни с цел да се фалшифицират данните на превозното средство (напр. пробег, скорост на движение, посока на движение и т.н.)
			20.5	Неупълномощени промени на данните за диагностика на системата
	21	Изтриване на данни/код	21.1	Неупълномощено изтриване/манипулиране на регистъра на събитията на системата
	22	Въвеждане на зловреден софтуер	22.2	Въвеждане на зловреден софтуер или активност на зловреден софтуер
	23	Въвеждане на нов софтуер или презаписване на съществуващ софтуер	23.1	Фалшифициране на софтуер на системата за управление на превозното средство или на информационната система
	24	Смущение на системи или операции	24.1	Отказ на услуги, например това може да бъде предизвикано във вътрешната мрежа чрез лавинна маршрутизация на шина CAN или като бъдат причинени грешки в електронен блок за управление чрез голям брой изпратени съобщения
	25	Манипулиране на параметрите на превозното средство	25.1	Неупълномощен достъп с цел фалшифициране на конфигурационните параметри на ключови функции на превозното средство, като например данни за спирачките, праг за разгънатата въздушна възглавница и т.н.
			25.2	Неупълномощен достъп с цел фалшифициране на параметрите за зареждане, като напрежение на зареждане, мощност на зареждане, температура на акумулатора и т.н.
4.3.7. Потенциални уязвимости, които може да бъдат използвани за атака, ако не са защитени в достатъчна степен	26	Криптографските технологии може да бъдат компрометирани или не са приложени в достатъчна степен	26.1	Комбинация от къси криптографски ключове и дълъг период на валидност позволява на атакуващия да дешифрира криптирането
			26.2	Недостатъчно използване на криптографски алгоритми, за да бъдат защитени чувствителните системи
			26.3	Използване на отхвърлени и подлежащи на отхвърляне криптографски алгоритми

Описание на високо равнище и подравнища на уязвимостите/заплахите			Пример за уязвимост или метод на атака	
	27	Част или доставки може да бъдат компрометирани, за да се осигури възможност за атакуване на превозни средства	27.1	Хардуер или софтуер, който е разработен, така че да осигури възможност за атака, или не отговаря на проектните критерии за спиране на атаки
	28	Уязвимости, възникнали при разработването на софтуера или хардуера	28.1	Софтуерни дефекти. Наличието на софтуерни дефекти може да бъде основа за потенциални уязвимости, осигуряващи възможност за атака. Това важи особено, ако софтуерът не е бил изпитан, за да се потвърди, че не е налице известен неправилен код/дефекти, и да се намали рискът от наличие на неизвестен неправилен код/дефекти
			28.2	Използването на остатъци от разработването (напр. портове за отстраняване на грешки, портове JTAG, микропроцесори, сертификати за разработване, пароли на разработчици...) може да осигури достъп до електронния блок за управление или да позволи на атакуващите да получат по-високи привилегии
	29	Структурата на мрежата представя уязвимости	29.1	Излишни интернет портове са оставени отворени, като предоставят достъп до мрежовите системи
			29.2	Заобикаляне на мрежовото разделяне, за да бъде получен контрол. Конкретен пример е използването на незащитени шлюзове или точки за достъп (като например шлюзове между камион и ремарке), за да бъдат заобиколени защитите и да бъде получен достъп до други мрежови сегменти с цел да бъдат извършени злонамерени действия, като например изпращане на произволни съобщения чрез шината CAN
	31	Може да възникне непредвидено предаване на данни	31.1	Компрометиране на информация. Може да има изтичане на лични данни при смяна на потребителя на колата (напр. продажба или използване като нает превозно средство с нови наематели)
	32	Физическо манипулиране на системите може да осигури възможност за атака	32.1	Манипулиране на електронен хардуер, напр. неодобрен електронен хардуер се добавя към превозно средство с цел да се осигури възможност за атака тип „посредник“ Замяна на одобрен електронен хардуеур (напр. датчици) с неодобрен електронен хардуер Манипулиране на информацията, събирана от датчик (например използване на магнит с цел да бъде нарушено функционирането на датчика на Хол, свързан със скоростната кутия)

Част Б. Мерки за смекчаване на заплахите, насочени към превозни средства.

1. Мерки за смекчаване, свързани с комуникационните канали на превозните средства

Мерките за смекчаване на заплахите, свързани с комуникационните канали на превозните средства, са изброени в таблица Б1.

Таблица Б1

Мерки за смекчаване на заплахите, свързани с комуникационните канали на превозните средства

Справка с таблицаА1	Заплахи, свързани с комуникационните канали на превозните средства	Спр.	Мярка за смекчаване
4.1	Фалшифициране на съобщения (напр. 802.11p V2X по време на групиране на превозни средства, съобщения от ГНСС и т.н.) чрез измама на основата на прилика	M10	Превозното средство проверява автентичността и валидността (целостта) на съобщенията, които получава
4.2	Атака Sybil (с цел да бъдат имитирани други превозни средства, за да се създаде впечатление, че на пътя има много превозни средства)	M11	Трябва да бъдат въведени контролни механизми за сигурност за съхранение на криптографските ключове (напр. използване на хардуерни модули за сигурност)
5.1	Комуникационните канали позволяват инжектиране на код в данните/кода на превозното средство, например подправени двоични софтуерни данни може да бъдат инжектирани в комуникационния поток	M10 M6	Превозното средство проверява автентичността и валидността (целостта) на съобщенията, които получава В системите трябва да бъде въведена сигурност още при разработването, за да бъдат сведени до минимум рисковете
5.2	Комуникационните канали позволяват манипулиране на данни/код, съхранявани на превозното средство	M7	Трябва да бъдат приложени техники и разработки за контрол на достъпа с цел да бъдат защитени данните/кодът на системите
5.3	Комуникационните канали позволяват презаписване на данни/код, съхранявани на превозното средство		
5.4 21.1	Комуникационните канали позволяват изтриване на данни/код, съхранявани на превозното средство		
5.5	Комуникационните канали позволяват въвеждането на данни/код в системите на превозното средство (запис на код от данни)		
6.1	Приемане на информация от ненадежден източник	M10	Превозното средство проверява автентичността и валидността (целостта) на съобщенията, които получава
6.2	Атака тип „посредник“/отвличане на сесията	M10	Превозното средство проверява автентичността и валидността (целостта) на съобщенията, които получава
6.3	Атака с повторно възпроизвеждане например атака срещу комуникационен шлюз позволява на атакуващият да върне по-старата версия на софтуера на електронен блок за управление или на софтуера на производителя на шлюза		
7.1	Прихващане на информация / смущаващи електромагнитни излъчвания / следене на комуникациите	M12	Трябва да бъдат защитени поверителните данни, предавани към или от превозното средство
7.2	Получаване на неупълномощен достъп до файлове или данни	M8	Структурата на системата и контролът на достъпа не трябва да позволяват неупълномощен персонал да получава достъп до лични данни или данни от критично значение за системата. Примери за контрол на сигурността може да бъдат открити в OWASP

Справка с таблицаA1	Заплахи, свързани с комуникационните канали на превозните средства	Спр.	Мярка за смекчаване
8.1	Изпращане на голям брой произволни данни към информационната система на превозното средство, така че да не може да предоставя услуги както при нормални условия	M13	Трябва да бъдат въведени мерки за откриване и възстановяване след компютърна атака тип „отказ на услуга“
8.2	Атака тип „черна дупка“ — нарушаване на комуникацията между превозните средства чрез блокиране на предаването на съобщения към други превозни средства	M13	Трябва да бъдат въведени мерки за откриване и възстановяване след компютърна атака тип „отказ на услуга“
9.1	Потребител без привилегии успява да получи привилегирован достъп, например достъп до кореновата файлова система	M9	Трябва да бъдат въведени мерки, за да се предотвратява и открива неупълномощеният достъп
10.1	Вирус, вграден в комуникационно устройство, инфектира системите на превозното средство	M14	Следва да бъде обмислено въвеждането на мерки, за да бъдат защитени системите срещу вградени вируси/зловреден софтуер
11.1	Зловредни вътрешни (напр. CAN) съобщения	M15	Следва да бъде обмислено въвеждането на мерки, за откриването на зловредни вътрешни съобщения или активност
11.2	Зловредни съобщения V2X, напр. инфраструктура към превозно средство или съобщения между превозни средства (напр. CAM, DENM)	M10	Превозното средство проверява автентичността и валидността (целостта) на съобщенията, които получава
11.3	Зловредни съобщения за диагностика		
11.4	Зловредни съобщения, обект на интелектуална собственост (напр. обичайно изпращаните от производител на оригинално оборудване или доставчик на компонент/система/функция)		

2. Мерки за смекчаване, свързани с процеса на актуализиране

Мерките за смекчаване на заплахите, свързани с процеса на актуализиране, са изброени в таблица Б2.

Таблица Б2

Мерки за смекчаване на заплахите, свързани с процеса на актуализиране

Справка с таблицаA1	Заплахи, свързани с процеса на актуализиране	Спр.	Мярка за смекчаване
12.1	Компрометиране на предавани по ефира процедури за актуализиране на софтуера. Това включва фалшифициране на програмата или софтуера на производителя за актуализиране на системата	M16	Трябва да бъдат въведени сигурни процедури за актуализиране на софтуера
12.2	Компрометиране на локални/физически процедури за актуализиране на софтуера. Това включва фалшифициране на програмата или софтуера на производителя за актуализиране на системата		
12.3	Софтуерът се подправя преди процеса на актуализиране (и следователно е компрометиран), макар че процесът на актуализиране не е засегнат		

Справка с таблицаA1	Заплахи, свързани с процеса на актуализиране	Спр.	Мярка за смекчаване
12.4	Компрометиране на криптографски ключове на доставчика на софтуер, за да се осигури възможност за невалидно актуализиране	M11	Трябва да бъде въведен контрол на сигурността по отношение на съхранението на криптографските ключове
13.1	Атака тип „отказ на услуга“ срещу сървър или мрежа за актуализиране с цел да се възпрепятства внедряването на актуализации на софтуера от критично значение и/или отключването на специфични за потребителя функции	M3	Трябва да бъде въведен контрол на сигурността по отношение на системите за данни и функционална логика. Когато сървъри за данни и функционална логика са от критично значение за осигуряването на услуги, съществуват мерки за възстановяване в случай на изключване на системата. Примери за контрол на сигурността може да бъдат открити в OWASP

3. Мерки за смекчаване, свързани с неумишлени човешки действия, които улесняват извършването на кибератака

Мерките за смекчаване на заплахите, свързани с неумишлени човешки действия, които улесняват извършването на кибератака, са изброени в таблица Б3.

Таблица Б3

Мерки за смекчаване на заплахите, свързани с неумишлени човешки действия, които улесняват извършването на кибератака

Справка към таблицаA1	Заплахи, свързани с неумишлени човешки действия	Спр.	Мярка за смекчаване
15.1	Невинна жертва (напр. собственик, оператор или инженер по поддръжката) е измамена да предприеме действие, така че непреднамерено да зареди зловреден софтуер или да осигури възможност за атака	M18	Трябва да бъдат въведени мерки за определяне и управляване на потребителските роли и привилегиите за достъп на основата на принципа за най-малко привилегии за достъп
15.2	Определените процедури за сигурност не се спазват	M19	Организациите трябва да гарантират, че са определени процедури за сигурност и че те се спазват, включително регистриране на действията и достъпа, свързани с управлението на функциите за сигурност

4. Мерки за смекчаване, свързани с външните връзки

Мерките за смекчаване на заплахите, свързани с външните връзки, са изброени в таблица Б4.

Таблица Б4

Мерки за смекчаване на заплахите, свързани с външните връзки

Справка с таблицаA1	Заплахи, свързани с външните връзки	Спр.	Мярка за смекчаване
16.1	Манипулиране на функции, предназначени за дистанционно управление на системи на превозното средство, като например ключове, имобилайзери и колони за зареждане	M20	Трябва да бъде въведен контрол по отношение на системите, които разполагат с дистанционен достъп
16.2	Манипулиране на телематиката на превозното средство (напр. манипулиране на измерването на температурата на чувствителни стоки, дистанционно отключване на товарните врати)		

Справка с таблицаA1	Заплахи, свързани с външните връзки	Спр.	Мярка за смекчаване
16.3	Смущаване на безжични връзки или датчици с малък обсег		
17.1	Компрометирани приложения или приложения с ниско ниво на сигурност на софтуера, използвани като метод за атакуване на системите на превозното средство	M21	Трябва да се извърши оценка на сигурността на софтуера, да се удостовери неговата автентичност и да се защити целостта му. Трябва да бъде въведен контрол на сигурността, за да се сведе до минимум рискът от софтуер от трета страна, който е предназначен или за който има вероятност да използва хостинг на превозното средство
18.1	Външни интерфейси като например USB или други портове, използвани като точка на атака — например чрез инжектиране на код	M22	Трябва да бъде въведен контрол на сигурността по отношение на външните интерфейси
18.2	Носител, който е заразен с вируси, е свързан към превозното средство		
18.3	Достъп за диагностика (напр. хардуерен ключ в порт OBD), използван за осигуряване на възможност за атака, напр. манипулиране на параметрите на превозното средство (пряко или непряко)	M22	Трябва да бъде въведен контрол на сигурността по отношение на външните интерфейси

5. Мерки за смекчаване, свързани с потенциалните цели или мотиви за компютърна атака

Мерките за смекчаване на заплахите, свързани с потенциалните цели или мотиви за компютърна атака, са изброени в таблица Б5.

Таблица Б5

Мерки за смекчаване на заплахите, свързани с потенциалните цели или мотиви за компютърна атака

Справка с таблицаA1	Заплахи, свързани с потенциалните цели или мотиви за компютърна атака	Спр.	Мярка за смекчаване
19.1	Извличане на защитен от авторско право или лицензиран софтуер от системите на превозното средство (пиратиране на продукт / кражба на софтуер)	M7	Трябва да бъдат приложени техники и разработки за контрол на достъпа с цел да бъдат защитени данните/кодът на системите. Примери за контрол на сигурността може да бъдат открити в OWASP
19.2	Неупълномощен достъп до поверителна информация на собственика, като например самоличност, информация за платежна сметка, информация от адресния указател, информация относно местоположението, електронен идентификатор на превозното средство и т.н.	M8	Структурата на системата и контролът на достъпа не трябва да позволяват неупълномощен персонал да получава достъп до лични данни или данни от критично значение за системата. Примери за контрол на сигурността може да бъдат открити в OWASP
19.3	Извличане на криптографски ключове	M11	Трябва да бъдат въведени контролни механизми за сигурност за съхранение на криптографските ключове, напр. модули за сигурност
20.1	Незаконни/неупълномощени промени на електронния идентификатор на превозното средство	M7	Трябва да бъдат приложени техники и разработки за контрол на достъпа с цел да бъдат защитени данните/кодът на системите. Примери за контрол на сигурността може да бъдат открити в OWASP
20.2	Използване на фалшива самоличност. Например, ако даден потребител иска да покаже друга самоличност, когато осъществява комуникация със системите за таксуване, сървъра за данни и функционална логика на производителя		
20.3	Действия за заобикаляне на системите за наблюдение (напр. хакерство/ подправяне/ блокиране на съобщения, като например данни от ODR Tracker, или брой изпълнения)	M7	Трябва да бъдат приложени техники и разработки за контрол на достъпа с цел да бъдат защитени данните/кодът на системите. Примери за контрол на сигурността може да бъдат открити в OWASP.

Справка с таблицаA1	Заплахи, свързани с потенциалните цели или мотиви за компютърна атака	Спр.	Мярка за смекчаване
20.4	Манипулиране на данни с цел да се фалшифицират данните на превозното средство (напр. пробег, скорост на движение, посока на движение и т.н.)		Компютърните атаки, свързани с манипулиране на данни от датчици или предавани данни, може да бъдат смекчени чрез съпоставяне на данните от различни източници на информация
20.5	Неупълномощени промени на данните за диагностика на системата		
21.1	Неупълномощено изтриване/манипулиране на регистъра на събитията на системата	M7	Трябва да бъдат приложени техники и разработки за контрол на достъпа с цел да бъдат защитени данните/кодът на системите. Примери за контрол на сигурността може да бъдат открити в OWASP.
22.2	Въвеждане на зловреден софтуер или активност на зловреден софтуер	M7	Трябва да бъдат приложени техники и разработки за контрол на достъпа с цел да бъдат защитени данните/кодът на системите. Примери за контрол на сигурността може да бъдат открити в OWASP.
23.1	Фалшифициране на софтуер на системата за управление на превозното средство или на информационната система		
24.1	Отказ на услуги, например това може да бъде предизвикано във вътрешната мрежа чрез лавинна маршрутизация на шина CAN или като бъдат причинени грешки в електронен блок за управление чрез голям брой изпратени съобщения	M13	Трябва да бъдат въведени мерки за откриване и възстановяване след компютърна атака тип „отказ на услуга“
25.1	Неупълномощен достъп с цел фалшифициране на конфигурационните параметри на ключови функции на превозното средство, като например данни за спирачките, праг за разгънатата въздушна възглавница и т.н.	M7	Трябва да бъдат приложени техники и разработки за контрол на достъпа с цел да бъдат защитени данните/кодът на системите. Примери за контрол на сигурността може да бъдат открити в OWASP
25.2	Неупълномощен достъп с цел фалшифициране на параметрите за зареждане, като например напрежение на зареждане, мощност на зареждане, температура на акумулатора и т.н.		

6. Мерки за смекчаване, свързани с потенциалните уязвимости, които може да бъдат използвани за атака, ако не са защитени в достатъчна степен

Мерките за смекчаване на заплахите, свързани с потенциалните уязвимости, които може да бъдат използвани за атака, ако не са защитени в достатъчна степен, са изброени в таблица Б6.

Таблица Б6

Мерки за смекчаване на заплахите, свързани с потенциалните уязвимости, които може да бъдат използвани за атака, ако не са защитени в достатъчна степен

Справка с таблицаA1	Заплахи, свързани с потенциалните уязвимости, които може да бъдат използвани за атака, ако не са защитени в достатъчна степен	Спр.	Мярка за смекчаване
26.1	Комбинация от къси криптографски ключове и дълъг период на валидност позволява на атакуващия да дешифрира криптирането	M23	Трябва да бъдат спазвани най-добрите практики в областта на киберсигурността за разработването на софтуер и хардуер

Справка с таблицаA1	Заплахи, свързани с потенциалните уязвимости, които може да бъдат използвани за атака, ако не са защитени в достатъчна степен	Спр.	Мярка за смекчаване
26.2	Недостатъчно използване на криптографски алгоритми, за да бъдат защитени чувствителните системи		
26.3	Използване на отхвърлени криптографски алгоритми		
27.1	Хардуер или софтуер, който е разработен, така че да осигури възможност за атака или не отговаря на проектните критерии за предотвратяване на атаки	M23	Трябва да бъдат спазвани най-добрите практики в областта на киберсигурността за разработването на софтуер и хардуер
28.1	Наличието на софтуерни дефекти може да бъде основа за потенциални уязвимости, осигуряващи възможност за атака. Това важи особено, ако софтуерът не е бил изпитан, за да се потвърди, че не е налице известен неправилен код/дефекти, и да се намали рискът от наличие на неизвестен неправилен код/дефекти	M23	Трябва да бъдат спазвани най-добрите практики в областта на киберсигурността за разработването на софтуер и хардуер. Изпитване на киберсигурността с подходящ обхват
28.2	Използването на остатъци от разработването (напр. портове за отстраняване на грешки, портове JTAG, микропроцесори, сертификати за разработване, пароли на разработчици...) може да позволи на атакуващия да получи достъп до електронния блок за управление или до по-високи привилегии		
29.1	Излишни интернет портове са оставени отворени, като предоставят достъп до мрежовите системи		
29.2	Заобикаляне на мрежовото разделяне, за да бъде получен контрол. Конкретен пример е използването на незащитени шлюзове или точки за достъп (като например шлюзове между камион и ремарке), за да бъдат заобиколени защитите и да бъде получен достъп до други мрежови сегменти с цел да бъдат извършени злонамерени действия, като например изпращане на произволни съобщения чрез шината CAN	M23	Трябва да бъдат спазвани най-добрите практики в областта на киберсигурността за разработването на софтуер и хардуер. Трябва да бъдат спазвани най-добрите практики в областта на киберсигурността за проектирането на системите и за системната интеграция.

7. Мерки за смекчаване, свързани със загуба на данни/компрометиране на данните от превозното средство

Мерките за смекчаване на заплахите, свързани със загуба на данни/компрометиране на данните от превозното средство, са изброени в таблица Б7.

Таблица Б7

Мерки за смекчаване на заплахите, свързани със загуба на данни/компрометиране на данните от превозното средство

Справка с таблицаA1	Заплахи, свързани със загуба на данни/ компрометиране на данните от превозното средство	Спр.	Мярка за смекчаване
31.1	Компрометиране на информация. Може да има изтичане на лични данни при смяна на потребителя на колата (напр. продажба или използване като наето превозно средство с нови наематели)	M24	По отношение на съхраняването на лични данни трябва да се спазват най-добрите практики за защита на целостта и поверителността на данните.

8. Мерки за смекчаване, свързани с физическо манипулиране на системите, което може да осигури възможност за атака

Мерките за смекчаване на заплахите, свързани с физическо манипулиране на системите, което може да осигури възможност за атака, са изброени в таблица Б8.

Таблица Б8

Мерки за смекчаване на заплахите, свързани с физическо манипулиране на системите, което може да осигури възможност за атака

Справка с таблицаА1	Заплахи, свързани с физическо манипулиране на системите, което може да осигури възможност за атака	Спр.	Мярка за смекчаване
32.1	Манипулиране на хардуера на производител на оригинално оборудване, напр. неразрешен хардуер се добавя към превозно средство с цел да се осигури възможност за атака тип „посредник“	M9	Трябва да бъдат въведени мерки, за да се предотвратява и открива неупълномощеният достъп

Част В. Мерки за смекчаване на заплахите извън превозните средства

1. Мерки за смекчаване, свързани със сървъри за данни и функционална логика

Мерките за смекчаване на заплахите, свързани със сървъри за данни и функционална логика, са изброени в таблица В1.

Таблица В1

Мерки за смекчаване на заплахите, свързани със сървъри за данни и функционална логика

Справка с таблицаА1	Заплахи, свързани със сървъри за данни и функционална логика	Спр.	Мярка за смекчаване
1.1 и 3.1	Злоупотреби с привилегии от страна на персонала (атака от вътрешно лице)	M1	Въвежда се контрол на сигурността по отношение на системите за данни и функционална логика, за да се сведе до минимум рискът от атака от вътрешно лице
1.2 и 3.3	Неупълномощен достъп чрез интернет до сървъра (което е било възможно например посредством задни вратички, некоригирани уязвимости на системния софтуер, атаки SQL или други средства)	M2	Въвежда се контрол на сигурността по отношение на системите за данни и функционална логика, за да се сведе до минимум рискът от неупълномощен достъп. Примери за контрол на сигурността може да бъдат открити в OWASP
1.3 и 3.4	Неупълномощен физически достъп до сървъра (извършен например чрез памет USB или друг носител, свързан към сървъра)	M8	Структурата на системата и контролът на достъпа не трябва да позволяват неупълномощен персонал да получава достъп до лични данни или данни от критично значение за системата
2.1	Атака срещу сървъра за данни и функционална логика прекратява неговото функциониране — например възпрепятства го да взаимодейства с превозни средства и да предоставя услуги, които са им необходими	M3	Въвежда се контрол на сигурността по отношение на системите за данни и функционална логика. Когато сървъри за данни и функционална логика са от критично значение за осигуряването на услуги, съществуват мерки за възстановяване в случай на изключване на системата. Примери за контрол на сигурността може да бъдат открити в OWASP.
3.2	Загуба на информация в изчислителния облак. Когато данните се съхраняват от доставчици на компютърни услуги „в облак“ трети страни, чувствителни данни може да бъдат загубени поради атаки или инциденти	M4	Въвежда се контрол на сигурността, за да се сведат до минимум рисковете, свързани с изчисленията в облак. Примери за контрол на сигурността може да бъдат открити в OWASP и насоките на NCSC относно изчисленията в облак
3.5	Нарушение на сигурността на информацията поради неумишлено споделяне на данни (напр. грешки на администратор, съхраняване на данни на сървъри в гаражи)	M5	Въвежда се контрол на сигурността по отношение на системите за данни и функционална логика с цел да се предотврати компрометирането на данни. Примери за контрол на сигурността може да бъдат открити в OWASP

2. Мерки за смекчаване, свързани с неумишлени човешки действия

Мерките за смекчаване на заплахите, свързани с неумишлени човешки действия, са изброени в таблица B2.

Таблица B2

Мерки за смекчаване на заплахите, свързани с неумишлени човешки действия

Справка с таблица-A1	Заплахи, свързани с неумишлени човешки действия	Спр.	Мярка за смекчаване
15.1	Невинна жертва (напр. собственик, оператор или инженер по поддръжката) е измамена да предприеме действие, така че непреднамерено да зареди зловреден софтуер или да осигури възможност за атака	M18	Трябва да бъдат въведени мерки за определяне и управляване на потребителските роли и привилегиите за достъп на основата на принципа за най-малко привилегии за достъп
15.2	Определените процедури за сигурност не се спазват	M19	Организациите трябва да гарантират, че са определени процедури за сигурност и че те се спазват, включително регистриране на действията и достъпа, свързани с управлението на функциите за сигурност

3. Мерки за смекчаване, свързани с физическа загуба на данни

Мерките за смекчаване на заплахите, свързани с физическа загуба на данни, са изброени в таблица B3.

Таблица B3

Мерки за смекчаване на заплахите, свързани с физическа загуба на данни

Справка с таблица-A1	Заплахи, свързани с физическа загуба на данни	Спр.	Мярка за смекчаване
30.1	Щети, причинени от трета страна. Чувствителни данни може да бъдат загубени или компрометирани поради физически щети в случай на пътнотранспортно произшествие или кражба	M24	По отношение на съхраняването на лични данни трябва да се спазват най-добрите практики за защита на валидността (целостта) и поверителността на данните. Примери за контрол на сигурността може да бъдат открити в ISO/SC27/WG5
30.2	Загуби поради конфликти, свързани с цифровото управление на права (DRM). Поради проблеми, свързани с цифровото управление на права, може да бъдат изтрити потребителски данни		
30.3	Чувствителни данни може да бъдат загубени или тяхната валидност (цялост) да бъде нарушена поради износване на ИТ компоненти което да причини потенциални проблеми с каскаден ефект (в случай например на изменение на ключове)		