

Проекти на наредби, представени пред Парламента съгласно параграф 8Е, точка 1 от приложение 7 към Закона за (оттегляне от) Европейския съюз от 2018 г и член 2, параграф 6, член 3, параграф 3, член 6, параграф 4, член 9, параграф 10, член 15, параграф 6 и член 77, параграф 5 от Закона за сигурността на продуктите и телекомуникациите от 2022 г., за одобрение с резолюция на всяка камара на Парламента.

ПРОЕКТ НА НОРМАТИВНИ ИНСТРУМЕНТИ

2023 г. №

ЗАЩИТА НА ПОТРЕБИТЕЛИТЕ

Наредби относно сигурността на продуктите и
телекомуникационната инфраструктура
(изисквания за сигурност за съответните продукти с
възможност за свързване)
от 2023 г.

Съставено - - - -

Влизане в сила - - 29 април 2024 г.

Държавният секретар изготвя настоящите наредби в изпълнение на правомощията, предоставени с член 8В от Закона за (оттеглянето от) Европейския съюз от 2018 г.^(а), и с член 1, параграф 1, член 3, параграф 1, член 6, параграф 1, член 9, параграф 3, буква б) и параграф 6, член 15, параграф 3 и член 77, параграф 2 от Закона за сигурността на продуктите и телекомуникациите от 2022 г.^(б).

Цитиране, влизане в сила и обхват

1. —(1) Тези наредби могат да бъдат цитирани като Наредби относно сигурността на продуктите и телекомуникационната инфраструктура (изисквания за сигурност за съответните продукти с възможност за свързване) от 2023 г.

(2) Настоящите наредби влизат в сила на 29 април 2024 г. и обхващат Англия и Уелс, Шотландия и Северна Ирландия.

Тълкуване

2. —(1) В настоящите Наредби:

„определен период на поддръжка“ означава минималният срок, изразен като период от време с крайна дата, за който ще се предоставят актуализации на защитата;

^(а) () 2018 г., гл. 16. Раздел 8В е добавен с раздел 21 от Закона за Европейския съюз (Споразумение за оттегляне) от 2020 г. (гл. 1).

^(б) () 2022 г., гл. 46.

„ETSI EN 303 645“ означава европейски стандарт за киберсигурност за потребителски интернет на нещата: Базови изисквания (ETSI EN 303 645 V2.1.1 (19 юни 2020 г.))(^a);

„хардуер“ означава физическа електронна информационна система или части от нея, с които могат да се обработват, съхраняват или предават цифрови данни;

„ISO/IEC 29147“ означава стандарт ISO/IEC 29147:2018 Информационни технологии. Методи за сигурност. Разкриване на уязвимост (2-ро издание, 2018 г.) (^b);

„предвидено от производителя предназначение“ означава употребата, за която е предназначен продуктът съгласно данните, предоставени от производителя, включително върху етикета, в инструкциите за употреба или в рекламни или търговски материали или твърдения;

„актуализация на защитата“ означава актуализация на софтуера, която защитава или повишава защитата на даден продукт, включително актуализация на софтуера, която решава проблеми със сигурността, които са били открити от или докладвани на производителя.

(2) Позоваванията в настоящите наредби на членове, освен ако не е посочено друго, се отнасят до членове от Закона за сигурността на продуктите и телекомуникационната инфраструктура от 2022 г.

(3) Други термини, използвани в настоящите наредби, имат значенията, посочени в член 56.

Изисквания за сигурност за производителите

3. В приложение 1 са посочени изискванията за сигурност, които се прилагат за производителите на съответните продукти с възможност за свързване за целите на член 1 (правомощия за определяне на изискванията за сигурност).

Определяне на съответствие с изискванията за сигурност

4. В приложение 2 са посочени условията, при които се счита, че даден производител е спазил изискване за сигурност за целите на член 3 (правомощия за определяне на съответствие с изискванията за сигурност).

Множество производители

5. Когато има повече от един производител на съответния продукт с възможност за свързване, всеки производител трябва да отговаря на съответните изисквания за сигурност, посочени в приложение 1, или да отговаря на условията за определяне на

^a (1) Европейски стандарт за киберсигурност за потребителски интернет на нещата: Базови изисквания (ETSI EN 303 645 V2.1.1 (19 юни 2020 г.)) е стандартът, определен от Европейския институт за стандарти в далекосъобщенията за стандартизация на киберсигурността на продуктите за потребителски интернет на нещата. Стандартът е достъпен безплатно на адрес https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf. Копие може също така да бъде разгледано безплатно след предварителна уговорка, като се свържете със Службата за безопасност на продуктите и стандарти на адрес Stanton Avenue, Teddington, Middlesex, TW11 0JZ или по електронна поща на адрес OPSS.enquiries@beis.gov.uk.

^b (1) Стандартът ISO/IEC 29147:2018 Информационни технологии. Методи за сигурност. Разкриване на уязвимост (2-ро издание, 2018 г.) е стандартът, определен от Международната организация за стандартизация, наред с други неща, за разкриване на уязвимост. Копие може да бъде разгледано безплатно след предварителна уговорка, като се свържете със Службата за безопасност на продуктите и стандарти на адрес Stanton Avenue, Teddington, Middlesex, TW11 0JZ или по електронна поща на адрес OPSS.enquiries@beis.gov.uk.

съответствие във връзка с това изискване в приложение 2.

Изключени продукти

6. В приложение 3 са посочени изключените продукти за целите на член 6 (изключени продукти).

Минимална информация, необходима за декларация за съответствие

7. В приложение 4 се посочва информацията, която трябва да се включи в декларацията за съответствие за целите на член 9 от (декларации за съответствие).

Запазване на декларацията за съответствие от производителя

8. Когато съгласно член 9, параграф 2 (декларации за съответствие) се изисква декларация за съответствие, за да се предостави съответен продукт с възможност за свързване в Обединеното кралство, производителят на продукта трябва да запази копие от декларацията за съответствие, отнасяща се до продукта, за по-дългия от следните периоди:

- (1) период от 10 години, започващ от датата на издаване на декларацията за съответствие, и
- (2) определения период на поддръжка за продукта, посочен в декларацията за съответствие.

Запазване на декларацията за съответствие от вносителя

9. Когато съгласно член 15, параграф 2 (декларации за съответствие) се изисква декларация за съответствие, за да се предостави даден продукт в Обединеното кралство, вносителят на продукта трябва да запази копие от декларацията за съответствие, отнасяща се до продукта, за по-дългия от следните периоди:

- (1) период от 10 години, започващ от датата на издаване на декларацията за съответствие, и
- (2) определения период на поддръжка за продукта, посочен в декларацията за съответствие.

Преглед

10.—(1) Държавният секретар трябва периодично:

- (1) да извършва преглед на нормативните разпоредби, съдържащи се в настоящите наредби; и
 - (2) да публикува доклад, в който са представени заключенията от прегледа.
- (2) Първият доклад трябва да бъде публикуван преди края на петгодишния период, считано от датата на влизане в сила на настоящите наредби.
- (3) Последващите доклади трябва да се публикуват през интервали, ненадвишаващи пет години;

Министър
Министерство на науката, иновациите и технологиите

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1

Наредба 3

Изисквания за сигурност за производителите

Пароли

1. —(1) Следните точки се прилагат за:

- (1) хардуер на продукта, когато този продукт не е във фабрично състояние по подразбиране;
- (2) софтуер, който е предварително инсталиран на продукта към момента, в който продуктът се доставя на даден клиент, когато продуктът не е в фабрично състояние по подразбиране;
- (3) софтуер, който не е предварително инсталиран на продукта към момента, в който продуктът се доставя на даден клиент, и който трябва да бъде инсталиран на продукта за всички предвидени от производителя предназначения на продукта, който използва:
 - (i) хардуер;
 - (ii) софтуер, който е предварително инсталиран към момента, в който продуктът се доставя на даден клиент; или
 - (iii) софтуер, който може да бъде инсталиран.
- (2) Паролите трябва да са:
 - (1) уникални за всеки продукт; или
 - (2) определени от потребителя на продукта.
- (3) Паролите, които са уникални за всеки продукт, не трябва да са:
 - (1) базирани на инкрементални броячи;
 - (2) базирани на или получени от публично достъпна информация;
 - (3) базирани на или получени от единни идентификационни кодове на продукти, като например серийни номера, освен ако това не е направено чрез използване на метод за криптиране или алгоритъм за хеширане с ключ, който се приема като част от добрите практики в сектора;
 - (4) лесни за отгатване.
- (4) В настоящия параграф паролите не включват:
 - (1) криптографски ключове;
 - (2) лични идентификационни номера, използвани за сдвояване в комуникационни протоколи, които не са част от пакета от интернет протоколи; или
 - (3) ключове за приложен програмен интерфейс.
- (5) В настоящия параграф:

„ключ за приложен програмен интерфейс“ означава низ от знаци, използвани за идентифициране и удостоверяване на конкретен потребител, продукт или приложение, така че да може да се осъществи достъп до приложения програмен интерфейс;

„криптографски ключ“ означава данни, използвани за криптиране и дешифриране на данни;

„фабрично състояние по подразбиране“ означава състоянието на продукта след възстановяване на фабричните настройки или след окончателното производство или сглобяване;

„добра практика в сектора“ означава упражняването на такава степен на умения, старание, предпазливост и предвидливост, каквато разумно и обичайно би се очаквала от квалифициран и опитен криптограф, който извършва същия вид дейност;

„инкрементален брояч“ означава метод за генериране на пароли, при който няколко пароли са еднакви с изключение на малък брой знаци, които се променят за всяка парола, за да я направят уникална (като например „password1“ и „password2“);

„алгоритъм за хеширане с ключ“ означава алгоритъм, който използва входящи данни („D“) и таен ключ („K“) за създаване на стойност, която не може да бъде отгатната или възпроизведена, без да се разполага с информация за D и K;

„таен ключ“ означава криптографски ключ, предназначен да бъде известен само на лицето („P“), което е криптирало или разрешило криптирането на данните, както и на всяко лице, упълномощено от P;

„уникален за всеки продукт“ означава уникален за всеки отделен продукт от даден продуктов клас или тип.

Информация за това как да се докладват проблеми със сигурността

2. —(1) Следните точки се прилагат за:

- (1) хардуер на продукта;
- (2) софтуер, който е предварително инсталиран на продукта към момента, в който продуктът се доставя на даден клиент;
- (3) софтуер, който трябва да бъде инсталиран на продукта за всички предвидени от производителя предназначения на продукта, който използва:
 - (i) хардуер;
 - (ii) софтуер, който е предварително инсталиран към момента, в който продуктът се доставя на даден клиент; или
 - (iii) софтуер, който може да бъде инсталиран;
- (4) софтуер, използван за или във връзка с предвидено от производителя предназначение на продукта, освен ако продуктът е смартфон или таблетен компютър с възможност за свързване към клетъчни мрежи.

(2) Трябва да се публикува следната информация:

- (1) най-малко едно звено за контакт, което да позволи на дадено лице („P“) да докладва на производителя проблеми със сигурността, свързани с категориите, изброени в точка 1, за всеки от съответните продукти с възможност за свързване на производителя, за които то има задължение съгласно член 8 (задължение за спазване на изискванията за сигурност); и
- (2) когато P ще получи:
 - (i) потвърждение за получаването на доклад за проблеми със сигурността; и

(ii) актуализиране на състоянието до разрешаването на докладваните проблеми със сигурността.

(3) Информацията по точка 2 трябва да бъде достъпна, ясна и прозрачна и трябва да бъде предоставена на Р:

- (1) без предварително искане за такава информация;
- (2) на английски език;
- (3) безплатно; и
- (4) без да се изисква предоставянето на лична информация на Р.

Информация за минималните периоди за актуализация на защитата

3. —(1) Следните точки се прилагат за:

(1) хардуер на продукта, който е в състояние да получава актуализации на защитата;

(2) софтуер, който е в състояние да получава актуализации на защитата, когато този софтуер е предварително инсталиран на продукта към момента, в който продуктът се доставя на даден клиент;

(3) софтуер, който е в състояние да получава актуализации на защитата, които трябва да бъдат инсталирани на продукта за всички предвидени от производителя предназначения на продукта, който използва:

(i) хардуер;

(ii) софтуер, който е предварително инсталиран към момента, в който продуктът се доставя на даден клиент; или

(iii) софтуер, който може да бъде инсталиран;

(4) софтуер, разработен от или от името на всеки производител, който е в състояние да получава актуализации на защитата и се използва за или във връзка с предвидено от производителя предназначение на продукта, освен ако продуктът е смартфон или таблетен компютър с възможност за свързване към клетъчни мрежи.

(2) Трябва да се публикува информация за определения период на поддръжка.

(3) Информацията по точка 2 трябва да бъде достъпна, ясна и прозрачна и трябва да бъде предоставена на дадено лице („Р“):

- (1) без предварително искане за такава информация;
- (2) на английски език;
- (3) безплатно;
- (4) без да се изисква предоставянето на лична информация на Р; и

(5) по такъв начин, който е разбираем за читател без предварителни технически познания.

(4) Когато производител публикува оферта за продажба на съответен продукт с възможност за свързване на своя уеб сайт или на неплатен уеб сайт под негов контрол, който съдържа информацията, описана в Наредба 6, параграф 4, буква а) от Наредбите от 2008 г., информацията в точка 2 трябва да бъде публикувана заедно с информацията, описана в тази наредба, или по друг начин да бъде отразена с еднакъв акцент.

(5) Изискванията за сигурност в настоящия параграф не са изпълнени, ако определеният период на поддръжка е съкратен след публикуването на информацията в

точка 2.

(6) Ако даден производител удължи минималния срок, за който ще се предоставят актуализации на защитата, като създаде нов определен период на поддръжка, информацията, свързана с новата определена поддръжка, трябва да бъде публикувана своевременно в съответствие с изискванията на точки 3 и 4.

(7) В настоящия параграф:

„Наредби от 2008 г.“ означава Наредби за защита на потребителите от нелоялна търговия от 2008 г.^(a);

„оферта за продажба“ има значението, дадено в Наредба 2, параграф 1 от Наредбите от 2008 г.

^{a)} S.I. 2021/1467.

Условия за определяне на съответствие с изискванията за сигурност

Пароли

1. —(1) Счита се, че даден производител отговаря на изискването за сигурност, посочено в параграф 1 от приложение 1, когато е изпълнено условието, посочено в точка 2.

(2) Условието е производителят да спазва разпоредба 5.1-1 от ETSI EN 303 645 и, когато е приложимо, разпоредба 5.1-2 от ETSI EN 303 645, когато тези разпоредби се прилагат за категориите хардуер и софтуер, посочени в параграф 1, точка 1 от приложение 1.

Информация за това как да се докладват проблеми със сигурността

2. (1) Счита се, че даден производител отговаря на изискването за сигурност, посочено в параграф 2 от приложение 1, когато е изпълнено условието, посочено в точка 2.

(2) Условието е производителят да спазва:

(1) разпоредба 5.2-1 от ETSI EN 303 645; или

(2) при спазване на точки 3 и 4, следните параграфи от ISO/IEC 29147:

(i) параграф 6.2.2;

(ii) параграф 6.5.2; и

(iii) параграф 6.5

когато разпоредбите на ETSI EN 303 645 или на параграфите от ISO/IEC 29147 се прилагат за категориите хардуер и софтуер, посочени в параграф 2, точка 1 от приложение 1.

(3) От даден производител се изисква да публикува информацията относно:

(1) как дадено лице може да получи достъп до механизма, позволяващ на производителя да получава докладите, описани в параграф 6.2.2 от ISO/IEC 29147;

(2) кога дадено лице, което изготвя доклад за уязвимост, ще получи потвърждение за получаване на доклад, описан в параграф 6.2.5 от ISO/IEC 29147; и

(3) кога дадено лице, което изготвя доклад за уязвимост, ще получи текуща комуникация, както е описано в параграф 6.5 от ISO/IEC 29147

(4) Информацията по точка 3 трябва да бъде достъпна, ясна и прозрачна и трябва да бъде предоставена на дадено лице („Р“):

(1) без предварително искане за такава информация;

(2) на английски език;

(3) безплатно; и

(4) без да се изисква предоставянето на лична информация на Р.

Информация за минималните периоди за актуализация на защитата

3. —(1) Счита се, че даден производител отговаря на изискването за сигурност,

посочено в параграф 1 от приложение 1, когато е изпълнено условието, посочено в точка 3.

(2) Условието е, при спазване на параграф 3, точки 4—6 от приложение 1 и на точки 3 и 4, производителят да спазва разпоредба 5.3-13 от ETSI EN 303 645, когато тази разпоредба се прилага за категориите хардуер и софтуер, посочени в параграф 3, точка 1 от приложение 1.

(3) Позоваванията в разпоредба 5.3-13 от ETSI EN 303 645 на „определен период на поддръжка“ следва да се тълкуват в съответствие с определението в Наредба 2.

(4) Позоваването в разпоредба 5.3-13 от ETSI EN 303 645 на информацията, която се публикува по достъпен, ясен и прозрачен начин, включва предоставянето на информация на дадено лице („Р“):

- (1) без предварително искане за такава информация;
- (2) на английски език;
- (3) безплатно;
- (4) без да се изисква предоставянето на лична информация на Р; и
- (5) по такъв начин, който е разбираем за читател без предварителни технически познания.

ПРИЛОЖЕНИЕ 3

Наредба 6

Изключени продукти с възможност за свързване

Продукти, предоставени за доставка в Северна Ирландия

1. (1) Продуктите се изключват съгласно настоящия параграф, ако са продукти, за които се прилага съответното законодателство и се предоставят за доставка в Северна Ирландия.

(2) За целите на настоящия параграф „съответно законодателство“ означава законодателство, което:

- (1) е включено в приложение 2 към Рамката от Уиндзор; и
- (2) при спазване на точка 3, съдържа член за свободно движение.

(3) Когато членът за свободно движение позволява на държавите членки, по причини, които не са свързани с аспекти, обхванати от съответното законодателство, да забраняват, ограничават или възпрепятстват предоставянето на продукта, когато продуктът отговаря на съответното законодателство, това законодателство трябва също така да разглежда аспектите, обхванати от приложение 1.

(4) В настоящия параграф:

„член за свободно движение“ означава член, с който не се позволява на държавите членки да забраняват, ограничават или възпрепятстват предоставянето на продукта, когато продуктът отговаря на това законодателство;

„Рамката от Уиндзор“ има същото значение като в Съвместна декларация № 1/2023 на ЕС и Обединеното кралство в Съвместния комитет по Споразумението за оттегляне от 24 март 2023 г.

Станции за зареждане на електрически превозни средства

2. —(1) Продуктите се изключват съгласно настоящия параграф, ако са станции за зареждане, за които се прилагат Наредбите от 2021 г.^(a).
- (2) Настоящият параграф има действие, все едно че Наредбите от 2021 г. обхващат Англия и Уелс, Шотландия и Северна Ирландия.
- (3) За целите на настоящия параграф позоваванията на „Великобритания“ в Наредба 3, параграф 2, буква б) от Наредбите от 2021 г. следва да се тълкуват като позовавания на „Обединеното кралство“.
- (4) В настоящия параграф:
- „Наредбите от 2021 г.“ означава Наредбите за електрически превозни средства (интелигентни станции за зареждане) от 2021 г.^(b);
- „станция за зареждане“ има значението, дадено в член 9, параграф 1 от Закона за автоматизираните и електрическите превозни средства от 2018 г.^(c).

Медицински изделия

3. —(1) Продуктите се изключват съгласно настоящия параграф, ако са продукти, за които се прилагат Наредбите за медицинските изделия от 2002 г.^(d)
- (2) Но съответен продукт с възможност за свързване, на който е инсталиран или може да се използва софтуер, за който се прилагат настоящите наредби, не е изключен продукт съгласно настоящия параграф.

Продукти за интелигентни измервателни уреди

4. —(1) Продуктите се изключват съгласно настоящия параграф, ако са продукти:
- (1) доставени или монтирани от или от името на лице, което действа в качеството си на притежател на лиценз съгласно:
- (i) член 7АБ от Закона за газа от 1986 г.^(e) (лицензиране на лице, предоставящо комуникационна услуга за интелигентни измервателни уреди); или
- (ii) член 6 от Закона за електричеството от 1989 г.^(f) (лицензи за разрешаване на доставки и др.); и
- (2) които са били успешно гарантирани в рамките на схема за гарантиране.
- (2) В настоящия параграф „схема за гарантиране“ означава схемата за гарантиране на търговски продукти, управлявана от Националния център за киберсигурност или от всяка друга схема правопреемник.

^a() S.I. 2021/1467.

^b() S.I. 2021/1467.

^c() 2018 г., гл. 18.

^d() S.I. 2002/618.

^e () 1986 г., гл. 44. Член 7АБ е добавен с Наредба 21 от Постановлението за електричество и газ (дейности по лицензиране на интелигентни измервателни уреди) от 2012 г. (S.I. 2012/2400).

^f () 1989 г., гл. 29. Съответните изменения на член 6 са направени с Наредба 6 от Постановлението за електричество и газ (дейности по лицензиране на интелигентни измервателни уреди) от 2012 г. (S.I. 2012/2400).

Компютри

5. —(1) Продуктите се изключват съгласно настоящия параграф, ако те са компютри, които са:

- (1) настолни компютри;
- (2) преносими компютри;
- (3) таблетни компютри, които нямат възможност да се свързват към клетъчни мрежи.

(2) Но продуктите, изброени в точка 1, които според предвиденото от производителя предназначение са предназначени изключително за деца под 14-годишна възраст, не са изключени продукти.

ПРИЛОЖЕНИЕ 4

Наредба 7

Минимална информация, необходима за декларациите за съответствие

1. —(1) Декларацията за съответствие трябва да включва следната информация:

- (1) продукт (тип, партида);
- (2) име и адрес на всеки производител на продукта и, когато е приложимо, на всеки упълномощен представител;
- (3) изявление, че декларацията за съответствие е изготвена от производителя на продукта или от негово име;
- (4) изявление, че по мнение на производителя са спазени:
 - (i) приложимите изисквания за сигурност в приложение 1; или
 - (ii) условия за определяне на съответствие в приложение 2;
- (5) определения период на поддръжка за продукта, който е бил правилен, когато производителят е доставил продукта за първи път;
- (6) подпис, име и длъжност на подписващото лице; и
- (7) мястото и датата на издаване на декларацията за съответствие.

(2) За целите на точка 1, буква г), подточка ii), когато позоваването включва съответствието на даден продукт с определен стандарт или спазването от страна на производителя на определен стандарт, идентификационният номер, версията и датата на издаване на стандарта трябва да бъдат включени в декларацията за съответствие, когато е приложимо.

ОБЯСНИТЕЛНА БЕЛЕЖКА

(Настоящата бележка не е част от наредбите)

С настоящите наредби се създават изисквания за сигурност за производителите на съответните продукти с възможност за свързване и се определят условията, които трябва да бъдат изпълнени, за да се счита, че дадено изискване за сигурност е спазено като част от регулаторния режим, посочен в част 1 от Закона за сигурността на продуктите и телекомуникациите от 2022 г. (гл. 46) („Закона“).

В настоящите наредби също така се определя кои продукти с възможност за свързване

се изключват от приложното поле на регулаторния режим и допълнително се определят изисквания във връзка с декларацията за съответствие за съответните продукти с възможност за свързване за производителите и вносителите.

В приложение 1 са посочени изискванията за сигурност, които производителите на съответните продукти с възможност за свързване трябва да спазват по отношение на потребителските продукти в Обединеното кралство.

В приложение 2 са посочени условията, при които, ако са изпълнени, ще се счита, че производителят отговаря на съответното изискване за сигурност.

В приложение 3 е посочен списъкът с продукти, които не се считат за съответни продукти с възможност за свързване за целите на член 4 от закона.

В приложение 4 е посочено минималното количество информация, което се изисква да бъде посочено в една декларация за съответствие.

Проект на настоящите наредби е нотифициран на Световната търговска организация съгласно задълженията на Обединеното кралство във връзка със Споразумението относно техническите пречки пред търговията **[да се въведе номер на нотификацията]**, както и на Европейската комисия съгласно Директивата за техническите стандарти и регламенти **[да се въведе номер на нотификацията]**.

Обяснителен меморандум е публикуван заедно с този инструмент на адрес www.legislation.gov.uk.