

НАРОДНО СЪБРАНИЕ
Вх. No 52-654-01-29
Дата 07.05 2026

ДО ПРЕДСЕДАТЕЛЯ

НА 52-ТО НАРОДНО СЪБРАНИЕ

Г-ЖА МИХАЕЛА ДОЦОВА

13¹⁹
[Signature]

УВАЖАЕМА ГОСПОЖО ПРЕДСЕДАТЕЛ,

На основание чл. 87 от Конституцията на Република България във връзка с чл. 70, ал. 1 т. 1 от временно действащия Правилник за организацията и дейността на Народното събрание, внасяме Законопроект за изменение и допълнение на Закона за киберсигурност.

Молим законопроектът да бъде представен за разглеждане и гласуване, съгласно установения ред.

ВНОСИТЕЛИ:

Костадин Костадинов
Сотко Томов Ангел
Петър Николов Петров
Коста Георгиев Стоянов
Исидор Лекайков Лекаев
Георги Николаев Георгиев
Димитър Георгиев Димитров
Ангел Ненов Георгиев
Кръстьо Стоянов Вразев
Ангел Василев Ангел
Борис Димитров Димитров

Ulaenun Tylbarob Tylbarob

Проект!

ЗАКОН
ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА
КИБЕРСИГУРНОСТ

(Обн. ДВ. бр.94 от 13 Ноември 2018г., изм. ДВ. бр.69 от 4 Август 2020г., изм. и доп. ДВ. бр.85 от 2 Октомври 2020г., изм. и доп. ДВ. бр.15 от 22 Февруари 2022г., изм. ДВ. бр.25 от 29 Март 2022г., изм. и доп. ДВ. бр.17 от 13 Февруари 2026г.)

§1. В чл. 27, ал. 1 и 2 се правят следните изменения и допълнения:

(1) Въз основа на информацията по чл. 26, ал. 2 Съветът по киберсигурността изготвя оценка на риска относно използването на технологии и вериги за доставка на ИКТ услуги и продукти от субектите по чл. 4 и 4а и при необходимост предлага на Министерския съвет мерки за управление и намаляване на установения риск.

(2) Мерките по ал. 1 могат да включват изисквания за допълнителни технически и организационни защити, диверсификация на доставчици, повишен мониторинг или други пропорционални действия, без да се въвежда обща забрана за използване на конкретни технологии, освен в изключителни случаи, свързани с доказан висок риск за националната сигурност.

§2. В чл. 27 се създава ал.3:

(3) Когато е установен висок риск, субектите по чл. 4 и 4а предприемат необходимите действия за неговото ограничаване в срок, определен с акта на Министерския съвет, съобразен с естеството и степента на риска.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§3. В срок до 6 месеца от влизането в сила на този закон Министерският съвет привежда подзаконовите нормативни актове в съответствие с него.

§4. Започнатите до влизането в сила на този закон процедури по ограничаване на използването на технологии се довършват съобразявайки се по този закон.

§5. В едногодишен срок от влизането в сила на този закон Съветът по киберсигурността извършва преглед на съществуващите решения и предложения, свързани с ограничаване на технологии, и при необходимост ги привежда в съответствие с подхода за управление на риска.

§6. Този закон влиза в сила от деня на обнародването му в „Държавен вестник“.

ВНОСИТЕЛИ:

Костадин Костадинов
Сотко Томов Анкер
Петър Николаев Петров
Коста Георгиев Саторджиев
Илира Михайлова Михайлова
Георги Николаев Георгиев
Димо Георгиев Димев
Ангел Ненов Георгиев
Владислав Стоянов Вразев
Ангел Василев Анкер
Борис Илиев Илиев
Иван Петров Петров

Мотиви

Към Законопроекта за изменение и допълнение на Закона за киберсигурност

С настоящия законопроект се предлага необходима реформа в закона за киберсигурност с цел да се постигне по-добър баланс между гарантирането на националната сигурност и създаването на предвидима, стабилна и благоприятна среда за развитие на цифровата икономика. В условията на ускорена дигитализация и нарастваща зависимост от информационни и комуникационни технологии, действащата уредба, която допуска широко ограничаване на използването на технологии, създава предпоставки за регулаторна несигурност, повишени разходи за бизнеса и риск от ограничаване на конкуренцията и иновациите. Това налага преминаване към по-гъвкав и съвременен подход, основан на оценка и управление на риска, който позволява прилагането на пропорционални и обосновани мерки в зависимост от конкретните обстоятелства.

С предложенията се цели привеждане на националната правна рамка в съответствие с изискванията на NIS2 Directive, като се въвежда модел, при който сигурността на мрежите и информационните системи се гарантира чрез системна оценка на рисковете, включително тези, произтичащи от веригите за доставки, и чрез прилагане на адекватни технически и организационни мерки. В този контекст ограничаването или преустановяването на използването на конкретни технологии се предвижда единствено като крайна мярка, приложима при доказан висок риск за националната сигурност или за функционирането на съществени услуги, когато по-леки мерки не биха били достатъчни. По този начин се осигурява съответствие с принципите на пропорционалност, необходимост и технологична неутралност, които са в основата на европейската регулаторна рамка.

Очакваният резултат от приемането на законопроекта е създаване на по-предвидима и устойчива регулаторна среда, която едновременно повишава нивото на киберсигурност и насърчава инвестициите и развитието на конкурентен пазар на ИКТ услуги. Чрез намаляване на възможностите за непропорционални ограничения и въвеждане на ясни критерии за държавна намеса се укрепва доверието на бизнеса и обществото в институциите, като

същевременно се гарантира ефективна защита на критичната инфраструктура и непрекъсваемост на основни услуги за гражданите и икономиката. Законопроектът отразява разбирането, че устойчивата киберсигурност следва да се постига чрез информирани, координирани и балансиращи решения, които съчетават интересите на сигурността, икономическото развитие и ангажиментите на Република България като държава членка на Европейския съюз.

ВНОСИТЕЛИ:

Костадин Костадинов

Сорго Томов Ангел

Петър Николаев Петров

Коста Георгиев Стоянов

Искра Михайлова Лиха

Георги НИКОЛАЕВ ГЕОРГИЕВ

Димитр Георгиев Дренев

Ангел Ненов Георгиев

Краско Стоянов Вразев

Ангел Василев Ангел

Борис Димитров Ангел

Ивелин Дарванов Дарванов

ПРЕДВАРИТЕЛНА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО

Към Законопроекта за изменение и допълнение на Закона за киберсигурност

1. Проблем, който се решава

Действащата уредба на чл. 27 предвижда възможност за ограничаване на използването на определени технологии и вериги за доставки, което може да доведе до прилагане на общи и непропорционални мерки, включително забрани, без достатъчно ясни критерии и без изрично изискване за оценка на риска.

Това създава предпоставки за:

- регулаторна несигурност;
- затруднения за субектите по закона при планиране на инвестиции;
- риск от ограничаване на конкуренцията;
- несъответствие с подхода на Европейския съюз, основан на управление на риска.

2. Цели на регулирането

Основната цел е въвеждане на подход, основан на оценка и управление на риска, който:

- гарантира високо ниво на киберсигурност;
- осигурява пропорционалност на мерките;
- повишава предвидимостта на регулаторната среда;
- съответства на изискванията на европейското право;
- запазва възможността за намеса при висок риск за националната сигурност.

3. Заинтересовани страни

Основните заинтересовани страни включват:

- субектите по чл. 4 и 4а (оператори на съществени и важни услуги);
- доставчици на ИКТ услуги и продукти;
- държавни органи, включително Съвета по киберсигурността;
- потребители на услуги от обществено значение;
- инвеститори и бизнес организации.

4. Варианти на действие

Вариант 0: Без действие

Запазване на действащата уредба.

Недостатъци:

- запазване на риска от непропорционални ограничения;
- ограничена съвместимост с NIS2 Directive;
- негативно въздействие върху инвестиционната среда.

Вариант 1: Предложен законопроект (предпочитан)

Въвеждане на подход, основан на оценка на риска и пропорционални мерки, като ограничаването на технологии се допуска само като крайна мярка.

Предимства:

- съответствие с европейското право;
- по-голяма гъвкавост;
- намаляване на административната тежест;
- подобрена предвидимост за бизнеса.

5. Очаквани въздействия

5.1 Икономически въздействия

- намаляване на регулаторната несигурност;
- подобряване на инвестиционния климат;
- стимулиране на конкуренцията;
- ограничаване на разходите, свързани с внезапни технологични промени.

5.2 Социални въздействия

- гарантиране на по-високо ниво на сигурност на услугите;
- запазване на достъпа до разнообразни и достъпни услуги;
- повишаване на доверието в публичните политики.

5.3 Въздействие върху бизнеса

- по-голяма предвидимост при планиране на инвестиции;
- възможност за гъвкаво управление на риска;
- намаляване на риска от внезапни забрани.

5.4 Административна тежест

- ограничено увеличение, свързано с извършване на оценки на риска;
- компенсирано от намаляване на тежестта при прилагане на рестриктивни мерки.

6. Въздействие върху държавния бюджет

Не се очаква значително въздействие върху държавния бюджет. Мерките ще се прилагат в рамките на съществуващите административни структури.

7. Съответствие с правото на ЕС

Предложението е съобразено с NIS2 Directive, като:

- въвежда управление на риска;
- отчита сигурността на веригите за доставки;
- прилага принципите на пропорционалност и необходимост;
- допуска ограничения само при доказан висок риск.

8. Рискове от прилагането

Възможни рискове:

- различно тълкуване на понятието „висок риск“;
- необходимост от допълнителен административен капацитет;
- забавяне при вземане на решения в сравнение с директни забрани.

Тези рискове се ограничават чрез:

- ясни критерии и процедури;
- координация на национално и европейско ниво;
- използване на съществуващи механизми за оценка.

9. Показатели за изпълнение

- брой извършени оценки на риска;
- брой приложени мерки за управление на риска;
- намаляване на инцидентите, свързани с вериги за доставки;
- степен на съответствие с европейските изисквания.

10. Заключение

Предложеният законопроект представлява балансирано решение, което повишава ефективността на политиките по киберсигурност, като същевременно създава предвидима и благоприятна среда за развитие на бизнеса и технологиите. Той е в съответствие с европейските изисквания и допринася за устойчивото развитие на цифровата икономика.

ВНОСИТЕЛИ:

Костадин Костадинов
Сокро Томов Пиле

Петър Николаев Петров

Коста Георгиев Стоянов

Искра Михайлов Михай

Георги Николаев Георгиев
Димитр Георгиев Дренев

Ангел Ненов Георгиев

Иринея Стоянов Врачев

Ангел Василев Ангел

Борис Димитров Ангелов

Ивелин Петров Петров