

НАРОДНО СЪБРАНИЕ	
Вх. №	52-654-01-87
Дата:	10 / 07 2026 г.

РЕПУБЛИКА БЪЛГАРИЯ

16 06
Сейф

ПЕТДЕСЕТ И ВТОРО НАРОДНО СЪБРАНИЕ

ДО

ПРЕДСЕДАТЕЛЯ НА

52-то НАРОДНО СЪБРАНИЕ

УВАЖАЕМА Г-ЖО ПРЕДСЕДАТЕЛ,

На основание чл. 87, ал. 1 от Конституцията на Република България и чл. 70, ал. 1, т. 1 от Правилника за организацията и дейността на Народното събрание, внасяме проект на Закон за допълнение на Закона за административното регулиране на икономическите дейности, свързани с нефт и продукти от нефтен произход, ведно с мотиви и предварителна оценка на въздействието към него.

Молим законопроектът да бъде представен за разглеждане и обсъждане по установения ред.

2026 г.

гр. София

ВНОСИТЕЛИ:

Борислав Ботанов
Георги Морфов

Александър Симеонов
Димитър Кайрезов
Васил Василев
Мария Димитрова
Силена Николова
Атанас Славов
Тимо Попов

Свистуны Урфоча

РЕПУБЛИКА БЪЛГАРИЯ
НАРОДНО СЪБРАНИЕ

Проект!

ЗАКОН

ЗА ДОПЪЛНЕНИЕ НА
ЗАКОН ЗА АДМИНИСТРАТИВНОТО РЕГУЛИРАНЕ НА
ИКОНОМИЧЕСКИТЕ ДЕЙНОСТИ, СВЪРЗАНИ С НЕФТ И
ПРОДУКТИ ОТ НЕФТЕН ПРОИЗХОД

(обн., ДВ, бр. 62 от 2018 г.; изм., бр. 13, 17 и 83 от 2019 г., бр. 9, 28 и 51 от 2020 г., бр. 15 от 2021 г., бр. 102 от 2022 г., бр. 8, 86 и 102 от 2023 г., бр. 70 от 2024 г. и бр. 97 от 2025 г., бр.55 от 2026г.)

§ 1. Създава се глава четвърта “б” с членове 27е-27з:

“Глава четвърта “б”.

Киберустойчивост на стратегически обекти

Чл. 27е. (1) Обектите на критична инфраструктура, представляващи стратегически обекти от значение за националната сигурност в сектор енергетика, предназначени за производство, преработка, обработка, съхраняване и пренос на нефт имат следните задължения за гарантиране на киберустойчивост:

1. изготвят подробен списък на компонентите на използвания от тях софтуер, хардуер, информационни системи и системи за индустриален контрол;
2. изготвят оценка на риска на доставчиците на активи по т. 1, базирана, включително на произхода на тези доставчици от трети страни с отчитане на съвместимостта с европейските стандарти за цифрова сигурност и устойчивост, по методика, утвърдена от председател на Държавна агенция “Национална сигурност”;
3. използват софтуер, хардуер, информационни системи и системи за индустриален контрол, които не представляват висок риск по смисъла на т. 2 за енергийната сигурност или непрекъсваемостта на дейността на съществен субект по смисъла на чл. 3, параграф 1, буква "а" от Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148;

4. уведомяват Държавна агенция "Национална сигурност" за планираното въвеждане в експлоатация на системи по т. 3 в тримесечен срок преди въвеждането в експлоатация;
 5. при поискване предоставят на Държавна агенция "Национална сигурност" оценката по т. 2 и списъка по т. 1.
- (2) Задълженията по ал. 1 се прилагат и по отношение на обекти и организации, които имат съществено влияние върху функционирането на обектите по ал. 1.
 - (3) Критични компоненти от списъка по ал. 1, т. 1, определени от Държавна агенция "Национална сигурност" функционират изолирано, без връзка с интернет и с други компютърни мрежи.
 - (4) Обектите и организациите по ал. 2 се определят от Държавна агенция "Национална сигурност";

Чл. 27ж. (1) При получаване на уведомление по чл. 27е, ал. 1, т. 4, Държавна агенция "Национална сигурност" предлага на групата за сътрудничество по смисъла на § 3, т. 2 от Закона за киберсигурност да бъде извършена Координирана на равнището на Европейския съюз оценка на риска за сигурността на критични вериги за доставка съгласно чл. 22 от Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 г. за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета (ОВ, L 333/164 от 27 декември 2022 г.) по отношение на активите по чл. 27е, ал. 1, т. 1.

- (2) При установен висок риск по ал. 1, обектите по чл. 27е, ал. 1 преустановяват използването или въвеждането в експлоатация на съответния актив по чл. 27е, ал. 1, т. 1.
- (3) Държавна агенция "Национална сигурност" изпраща на Народното събрание доклади за получените уведомления, предложението за извършване на оценка на риска и резултата от извършената оценка на риска.

Чл. 27з. (1) Държавна агенция "Национална сигурност" извършва проверки в обектите по чл. 27е, ал. 1 веднъж на всеки 6 месеца, като проверките имат най-малко следния обхват:

1. проверка на списъка по чл. 27е, ал. 1, т. 1;
 2. проверка на оценката на риска по чл. 27е, ал. 1, т. 2;
 3. проверка на предприетите организационни и технически мерки за гарантиране на нивото на киберсигурност;
- (2) При извършването на проверките по ал. 1, ръководителите на обектите по чл. 27е, ал. 1 осигуряват пълен достъп до помещенията, документацията и техническите експерти в сферата на информационните технологии.
 - (3) Докладът от проверката по ал. 1 се изпраща до министър-председателя, министъра на икономиката, инвестициите и индустрията, министъра на енергетиката и до съответните парламентарни комисии, както и до парламентарната комисия, която осъществява контрол върху дейността на службите за сигурност.

§ 2. Създава се чл. 33а:

“Чл. 33а. Който не изпълни задълженията по глава четвърта “б” се наказва с глоба или имуществена санкция от 20 000 до 200 000 лв.

§ 3. В чл. 36 се създава нова ал. 6:

“(6) Актовете за установяване на административните нарушения по чл. 33а се съставят от оправомощени от председателя на Държавна агенция “Национална сигурност” длъжностни лица, а наказателните постановления се издават от председателя на Държавна агенция “Национална сигурност” или оправомощен от него заместник.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 4. Председателят на Държавна агенция “Национална сигурност” приема методиката по чл. 27е, ал. 1, т. 2 в тримесечен срок от обнародването на този закон в Държавен вестник.

§ 5. В едногодишен срок от влизането в сила на този закон, организациите, опериращи обекти по чл. 27е, ал. 1:

1. прилагат чл. 27е, ал. 1, т. 2 по отношение на всички въведени в експлоатация активи;
2. изпращат на Държавна агенция “Национална сигурност” информация за съществуващия софтуер, хардуер, информационни системи и системи за индустриален контрол, като Държавна агенция “Национална сигурност” прилага чл. 27ж, ал. 1.

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

ВНОСИТЕЛИ:

Богдан Богданов
Пламен Морави

Александър Сиднев
Димитър Вайценов
Стефан Стефанов
Мария Димитров
Силена Ангелова
Атанас Савов
Емил Попов
Светен Мирков

МОТИВИ

Към Законопроект за допълнение на Закона за административното регулиране на икономическите дейности, свързани с нефт и продукти от нефтен произход

Обектите на критична инфраструктура, вкл. тези, представляващи стратегически обекти от значение за националната сигурност в сектор енергетика, предназначени за производство, преработка, обработка, съхраняване и пренос на нефт (петролните рафинерии) са под особен риск във връзка на използваните от тях софтуер, хардуер, информационни системи и системи за индустриален контрол, когато те са произведени от производител от трета страна съответно оценен като такъв с висок риск.

Множество са възможните кибератаки, вкл. чрез “задни вратички”, чрез веригата на доставки и др. И докато по отношение на организации, които не представляват стратегически обекти, този риск може да бъде приет, то по отношение на стратегически обекти той е недопустим, с оглед на множеството асоциирани рискове: спиране на работата, забавяне на работата, промяна на важни формули и съотношения, саботаж, вкл. човешки жертви и материални щети.

Особената обществена значимост на тези обекти произтича не само от тяхната роля в енергийния сектор, но и от прякото им значение за националната сигурност, икономическата стабилност и непрекъсваемостта на доставките на нефт и продукти от нефтен произход. Нарушаването на нормалното функциониране на подобна инфраструктура може да има последици, които надхвърлят обичайните рискове за отделен стопански субект и да засегнат обществения ред, сигурността на снабдяването, дейността на други критични сектори и защитата на живота и здравето на гражданите. Поради това въвеждането на специални превантивни изисквания към използваните технологични активи и към риска, произтичащ от веригите на доставки, е оправдано, необходимо и пропорционално на преследваната цел.

От тази гледна точка, с настоящия законопроект се предлагат нарочни мерки за повишаване на киберустойчивостта на рафинерии чрез набор от мерки, свързани с анализ на риска при използваните софтуер, хардуер, информационни системи и системи за индустриален контрол.

Мерките включват забрана за използване на високорискови технологии, като оценката на риска е на две нива - първото ниво е вътрешно (проведено от самата организация, по методика на ДАНС), а второто ниво е координирана на ниво ЕС оценка на риска, по инициатива на ДАНС. Във всеки от двата случая използването на дадена технология следва да бъде преустановено, а нова такава да не бъде въведена в експлоатация.

Заварените системи също подлежат на такава оценка в 12-месечен срок от влизането в сила на закона, като по този начин ще бъде постигната в максимална степен устойчивост на редица киберрискове.

ВНОСИТЕЛИ:

Борислав Борисов
Наско Насков

Александър Сидишев
Димитър Клейчев
Осипо Косичев
Марин Димитров
Стефан Николов
Атанас Славев
Томас Попов
Светлин Турфанчев

РЕПУБЛИКА БЪЛГАРИЯ

ПЕТДЕСЕТ И ВТОРО НАРОДНО СЪБРАНИЕ

**ПРЕДВАРИТЕЛНА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО НА
ПРОЕКТА НА ЗАКОН ЗА ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА
АДМИНИСТРАТИВНОТО РЕГУЛИРАНЕ НА ИКОНОМИЧЕСКИТЕ ДЕЙНОСТИ,
СВЪРЗАНИ С НЕФТ И ПРОДУКТИ ОТ НЕФТЕН ПРОИЗХОД**

I. Част първа

Елементи на оценката	Аргументация
Основания на законодателната инициатива	Основание за законодателната инициатива е необходимостта от въвеждане на специални превантивни мерки за ограничаване на киберрисковете по отношение на стратегически обекти от значение за националната сигурност в сектор „Енергетика“, свързани с производство, преработка, обработка, съхраняване и пренос на нефт. С оглед на критичното значение на тези обекти за енергийната сигурност, обществения ред, икономическата стабилност и непрекъсваемостта на доставките, използването на високорискови софтуер, хардуер, информационни системи и системи за индустриален контрол създава недопустим риск от прекъсване, саботаж или компрометиране на дейността им. Предлаганите допълнения имат за цел да осигурят навременна идентификация, оценка и ограничаване на този риск чрез въвеждане на допълнителни изисквания за киберустойчивост и контрол върху технологичните активи и веригите на доставки.
Заинтересовани групи	Заинтересовани страни са операторите на стратегически обекти в сектор „Енергетика“, свързани с нефт и продукти от нефтен произход, компетентните органи в областта на националната сигурност и киберсигурността, доставчиците на технологични активи и услуги, както и гражданите и бизнесът като крайни ползватели на енергийната сигурност и непрекъсваемостта на доставките.
Анализ на разходи и ползи	Не се очакват допълнителни административни разходи, тъй като не се правят промени водещи до такива разходи.

Елементи на оценката	Аргументация
Административна тежест и структурни промени	Не се предвиждат и не са необходими административни промени, като закриване, сливане или създаване на нови административни структури.
Въздействие върху нормативната база	Предлаганите промени изискват приемане на подзаконов акт методика, утвърдена от председателя на Държавна агенция „Национална сигурност“, с която да се определят критериите и редът за извършване на оценка на риска на доставчиците на софтуер, хардуер, информационни системи и системи за индустриален контрол. Не се налагат други изменения в действащата нормативна уредба.
Равно третиране от държавата и балансирано демографско развитие	Предложението не засяга спазването на принципа на равенство съгласно българското законодателство и за равното третиране от държавата на българите и българските граждани, живеещи извън страната.

ВНОСИТЕЛИ:

Борислав Борисков
Натанел Мързев

Александър Сиднев
Христо Христов
Васил Василев
Мария Димитрова
Силена Николова
Атанас Славов
Тимо Попов
Светлин Трънчев