НАРОДНО СЪБРАНИЕ
Вх.No 51-554-04-136
Дата 17 / 03 2025 г.

РЕПУБЛИКА БЪЛГАРИЯ
ПЕТДЕСЕТ И ПЪРВО НАРОДНО СЪБРАНИЕ

ЧРЕЗ
ПРЕДСЕДАТЕЛЯ НА
51-ОТО НАРОДНО СЪБРАНИЕ
НАТАЛИЯ КИСЕЛОВА

ДО
ПРЕДСЕДАТЕЛЯ НА
КОМИСИЯТА ПО ЕЛЕКТРОННО УПРАВЛЕНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ
ЛЕВЕНТ МЕМИШ

УВАЖАЕМИ Г-Н ПРЕДСЕДАТЕЛ,

На основание чл. 79, ал.1 от Правилника за организацията и дейността на Народното събрание, правим следните мотивирани изменения и допълнения в Законопроекта за изменение и допълнение на Закона за киберсигурност (51-402-01-17):

1. В § 3, т. 4 думите "по предложение на Комисията за регулиране на съобщенията и на министъра на електронното управление" се заменят с думите "по предложение на министъра на електронното управление съгласувано с Комисията за регулиране на съобщенията"

Мотиви: Не е обичайна практика независими регулатори да предлагат на Министерския съвет да приема наредби. Обикновено ресорното министерство изготвя съвместно с регулатора проекта на наредба и я предлага на Министерския съвет.

2. В § 4, в чл. 4, т. 6 след думите "от критично значение" се добавят думите "в секторите по Приложение I"

Мотиви: текстът по вносител е с недостатъчно ясен обхват, което създава и неяснота при прилагането. Поради това се предлага уточнение за секторите, в които законът се прилага спрямо научноизследователската дейност.

3. В § 5 относно чл. 4а се създава ал. 3:
(3) Министърът на електронното управление публикува списък с кодове по Класификацията на икономическите дейности, утвърдена от Националния статистически институт, с които се класифицира дейността на съществените и важните субекти;

Мотиви: С цел улеснение на критичните и важните субекти по отношение на разумното очакване за включването им в регистъра на съответния вид субекти, следва МЕУ да изготви и публикува списък с кодове по КИД, които да обвърже със секторите в приложенията на този закон.

4. В § 6, т. 1 и т. 2 се отменят, а т. в т. 3 думите "4 и 5" се заменят с думите "3, 4 и 5"

Мотиви: Няма основание Комисията за противодействие на корупцията да бъде изключена от обхвата на закона.
Няма основание и конкретни системи в стратегически обекти да не подлежат на контрол - това потенциално може да бъде несъответствие с директивата, тъй като много от стратегическите обекти и дейности са в обхвата на директивата. С решение на МС може да бъде определен ДАНС за Национален компетентен орган по отношение на тези субекти или конкретно на тези системи. В допълнение, не може наредба да се реферира по име в закон, а трябва да бъде цитирана разпоредбата, на чието основание е приета.

5. В §14 се правят следните изменения и допълнения:
а) В т. 5, т. 9 се изменя така:
"9. осъществява проверки на предоставените одитни доклади от националните компетентни органи по ред, определен в наредбата по чл 3, ал. 2.

б) създава т. 6:
"6. Създава се т. 10-13:
"10. организира провеждането на тестове за проникване в информационни системи и мрежи, които не са защитени по реда на Закона за достъп до класифицирана информация;
11. определя ограничения за използване на приложения и интернет страници на служебните устройства на държавните служители;
12. получава от компетентните органи, обобщава и публикува списъци с интернет адреси и други данни, подавани към производители и доставчици на ИКТ продукти и ИКТ услуги за киберсигурност, свързани с ограничаване на достъпа до интернет адреси, свързани със злонамерено поведение;
13. координира участието на България в групата за сътрудничество;
14. е национален орган за сертифициране по Регламент (ЕС) 2019/881;
15. приема наредба за реда и условията за сертифициране по Регламент (ЕС) 2019/881"

Мотиви: Регулярното организиране на тестове за проникване е ключово за поддържане на ниво на киберсигурност. Липсата на законов текст създава организационни пречки пред ефективното организиране на такива тестове.
С т. 11 се предлага възможност за прилагане на на ограничения за използване от страна на държавни служители на определени рискови приложения или уеб сайтове. Напр. tiktok е ограничен за ползване от държавни служители в някои партньорски държави, както и в ЕС. Друг пример е забраната за използване на онлайн хазарт, който традиционно е забранен в корпоративни мрежи.

С т. 12 се предлага МЕУ да обобщава адреси и други индикатори, подадени от органите (ГДБОП, ДАНС, други) към производителите на софтуер за киберсигурност за включване в т.нар. "черни списъци".

6. Създава се § 14а:
§ 14а. В чл. 13, ал. 2 се създава т. 4:
"4. организира изграждането и развиването на способности за офанзивни кибер операции;"

Мотиви: значителното увеличение на кибератаките от киберпрестъпниците и подкрепяните от неприятелски държави хакерски групи нанасят все повече щети и се използват за постигане на политически цели. Както видяхме в последните години киберпространството е петият домейн за водене на война, къде дори и в мирно време се извършва разузнаване на инфраструктурата на потенциални бъдещи неприятелски държави, извършват се саботажи и др. Изграждането на т.нар. "офанзивни кибер операции", чрез които да бъде отслабена инфраструктурата на атакуващите значително ще намали тяхната ефективност. В нормална обстановка развитият капацитет може да се използва и за т.нар. "red teaming" - практика, при която се прави опит за проникване в собствените мрежи и с която се постига значително увеличаване на киберсигурността на организациите, участващи в упражнението.

7. В § 15 накрая се добавят думите "а накрая се добавят изречение второ и трето:
"Уведомленията по предходното изречение се съгласуват с Министерството на електронното управление по ред, определен в наредбата по чл. 3, ал. 2. В случай на отрицателно становище от Министерството на електронното управление, преустановеният достъп се възстановява. Министерството на вътрешните работи представя на ресорната комисия в Народното събрание доклад за извършените действия по преустановяване на интернет трафик веднъж на всеки три месеца."

Мотиви: в това правомощие на МВР може да има потенциални злоупотреби в случай, че липсва междуинституционален взаимен контрол, поради което следва да има съгласуване. Съгласуването може да е пост-фактум, поради времево-чувствителния характер на процеса, като подробностите по процеса на съгласуване следва да бъдат уредени в наредба. Тъй като блокирането на интернет трафик е обществено чувствителна тема, се предвижда веднъж месечно да се представят доклади пред Народното събрание за блокираните адреси.

8. В § 16 се създават ал. 8 и 9:

"(8) Държавна агенция „Национална сигурност" приема специфичните изисквания към киберсигурността в организациите по ал. 1 след съгласуване със Съвета по киберсигурност.
(9) Веднъж годишно Държавна агенция „Национална сигурност" предоставя на Съвета по киберсигурност доклад за изпълнението на изискванията на този закон от в организациите по ал. 1"

Мотиви: Чрез въвеждането на ясни изисквания към стратегически обекти и възлагащите и извършващите стратегически дейности от значение за националната сигурност се дава възможност за планиране на изграждането и подобрението на киберсигурността в тези организации, създава се възможност за обективна оценка на спазването на мерките за киберсигурност, включително и на национално ниво.

9. В §17 се правят следните допълнения:
а) в т. 2 накрая се добавят думите: "и се добавя изречение второ: "Министерството на електронното управление е и национален компетентен орган за всички сектори и услуги, посочени в приложения № 1 и 2, за които не е определен такъв със закон или с решение по ал. 1"

б) създава се ал. 14-15:
"(14) Националните компетентни представят на министъра на електронното управление одитни доклади за дейността си веднъж годишно по ред, определен в наредбата по чл 3, ал. 2.
(15) Министърът на електронното управление извършва преглед на дейността на националните компетентни органи, в т.ч. чрез проверка на одитните им доклади. В случай, че установи системно неизпълнение на задълженията, министърът на електронното управление предлага на Министерския съвет изменение на решението по ал. 1"

Мотиви: С предложенията МЕУ се определя за НКО за всички сектори, освен ако не са определени други с решение - това позволява изграждане на капацитет за контролна дейност, какъвто към момента е силно ограничен. Развиването на множество НКО рискува те да са само документално такива, но да не извършват реална дейност поради липса на капацитет. За да се избегнат такива случаи, се предвижда МЕУ да контролира всички НКО и да предлага тяхното изваждане от решението по ал. 1, в случай, че те системно не изпълняват задълженията си по този закон.

10. В §18 се правят следните изменения и допълнения:
а) т. 1 се отменя
б) създава се т. 12:
"12. Създава се ал. 14:
(14) Функциите на НЕЗК се изпълняват от НЕРИКС, освен ако министърът на електронното управление не определи друго звено за НЕЗК"

Мотиви: Редакционното предложение по т. 1 не е необходимо, тъй като нормативните актове създават права и задължения, а не отчитат исторически факти за създаването на завена и системи.
С новата т. 14 се обединяват функциите на НЕРИКС и НЕЗК, тъй като двете звена трябва да работят в много тясна координация, вкл. по отношение на международните контакти. Изпълнението на функциите на НЕЗК от НЕРИКС ще улесни координацията, без да наруши основни принципи в директивата.

11. В §23, в ал. 1 думите "може да изпрати" се заменят с думите "или оправомощено от него лице, както и ръководителите на СЕРИКС и НЕРИКС могат да изпратят"

Мотиви: Исканията до групата за сътрудничество за извършване на партньорска проверка следва да могат да се изпращат и от оправомощени от него лица - напр. директора на ресорната дирекция, ресорен заместник-министър, главния секретар. Отделно от това, всеки ЕРИКС следва да има право да поиска такава партньорска проверка, тъй като тя е именно за съответствие на ЕРИКС.

12. В §25, чл. 23 се създават ал. 13-15:
"(13) С наредбата по чл. 3, ал. 2 могат да бъдат определи и други категории инциденти, които подлежат на докладване към ЕРИКС и за които трябва да се изпраща информация до националното единно звено за контакт по реда на този член.
(14) Компетентните органи по Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 година относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 уведомяват НЕРИКС за докладвани към тях съществени инциденти с ИКТ
(15) Информация за киберинцидентите се съхранява и обменя чрез системите по чл. 27г, ал. 6."

Мотиви: Въвеждане на координация при докладването на инциденти между компетентните органи по NIS2 и DORA.
С ал. 13 се предвижда възможност за разширяване на докладването към СЕРИКС и НЕРИКС на други инциденти, чието докладване би било от полза за общото ниво на киберсигурност, но които не са критични.
С ал. 15 се въвежда задължение за обмен на данни и тяхното съхранение чрез системата на МЕУ за информация за киберзаплахи, като това включва т.нар. индикатори за компрометиране. Към момента има изградени необходимите системи, като следва те да получат своята институционализация и задължителен характер.

13. В §25, чл. 24, ал. 1 думите "НКО след одобрението на Съвета по киберсигурността може да изиска от" се заменя с думите "Министерският съвет с постановление, прието по предложение на съвета по киберсигурност, може да създаде изисквания за"

Мотиви: Поради сериозността на това правомощие, водещо до налагане на конкретни технологични изисквания, решения за налагане на конкретни технологии следва да имат нормативен характер и да подлежат на обществено обсъждане, поради което следва да се приемат чрез постановления на Министерския съвет.

14. В §25 се създават чл. 26 и чл. 27:
Координирана на равнището на Съюза оценка на риска за сигурността на критични вериги за доставка
Чл. 26. (1) Министърът на електронното управление може да инициира Координирана на равнището на Съюза оценка на риска за сигурността на критични вериги за доставка.
(2) Министърът на електронното управление представя резултатите от координираната проверка на Съвета по киберсигурност.

Ограничаване на използването на рискови технологии
Чл. 27. (1) Съветът по киберсигурността идентифицира и прави оценка на технологичните и нетехнологичните рискове, като изготвя мотивирано предложение до Министерския съвет за приемане на постановление за ограничаване на използването от субектите по чл. 4 и чл. 4а на конкретни технологии или на критични вериги за доставка на ИКТ услуги и ИКТ продукти, с произход от страни извън Европейския съюз, доколкото с това не се засягат императивни разпоредби на правото на Европейския съюз или на действащото българско законодателство и не се влиза в противоречие с координираните оценки на риска в рамките на Европейския съюз.
(2) В случай, че субектите чл. 4 и чл. 4а вече изпозлват технология, която е ограничение с постановлението по ал. 1, те имат срок от две години да преустановят използването на съответната технология, освен в случаи на висок риск за националната сигурност.

Мотиви: Предложението в чл. 27 е необходимо, за да може да се ограничи използването на конкретни технологични производители, за които има данни, че могат да окажат влияние на националната киберсигурност чрез изтичане на данни или въздействие на чужди правителства. Към настоящият момент организациите в обхвата на ЗОП нямат мерки, ако подобен доставчик, дотиран от собствената си държава, предложи занижена цена на технология или услуга. Други европейски държави, като Румъния например, са приели подобни мерки, позволяващи им да спират навлизането на конкретни технологични производители

15. §26 се отменя

Мотиви: параграф 26 отменя чл. 26 и 27, като с оглед на предложенията по т. 14, те не следва да бъдат отменяни.

16. В §28 по отношение на чл. 27г се създават ал. 5-6:
“(5) Обменът на информация по ал. 1 е задължителен за държавните органи и публичните предприятия и се осъществява по ред, определен в наредбата по чл. 3, ал. 2.
(6) Министърът на електронното управление изгражда и поддържа информационни системи за съхранение и автоматизиран обмен информацията по ал. 1

(7) Информацията по ал. 1, която подлежи на съхранение в системите по ал. 6 в структуриран вид, не се създава като класифицирана информация."

Мотиви: обменянето на информация за киберзаплахи (т.нар. индикатори на компрометиране) е добра практика и тя следва да е задължителна поне за държавните органи и публичните предприятия, за да има достатъчно пълна база данни. Към момента има изградени такава система, като следва те да получат своята институционализация и задължителен характер. Такива системи за системата за обмен на киберразузнавателна информация, базата данни с уязвимости, базата данни с известни вируси.
С ал. 7 се въвежда забрана за свръхкласифициране на информация, каквато тенденция е имало през годините, по отношение на киберразузнавателна информация. Добрата практика изисква конкретните индикатори за компрометиране в структуриран вид (IP адреси, имейли, хешове на вируси и др.) да бъдат явни, а при нужда, контекстът да бъде класифициран - как са придобити, какви са били целите на киберзаплахите/инцидентите и др. Класифицирането на този вид информация я прави безполезна, тъй като тя трябва да се поддържа в явни системи.

17. В §29:
а) В чл. 27ж се създава ал. 4:
"(4) Органите по чл. 27е осъществяват дейностите по ал. 1 спрямо определен субект не по-рано от шест месеца от вписването на съответния субект в регистъра по чл. 6."
б) В чл. 27и се създава нова ал. 3:
"(3) Органите по чл. 27е издават актовете по ал. 1 спрямо определен субект не по-рано от шест месеца от вписването на съответния субект в регистъра по чл. 6."

Мотиви: С предложението се предвижда период от 6 месеца за привеждане на дейността на съответния субект в съответствие с този закон от вписването му в регистъра, т.е. от определянето му като задължен субект по този закон. В противен случай се създава риск от прекомерна административна тежест - проверка за съответствие и санкционна дейност без предизвестие от момента, в който дадено лице става задължен субект.

18. В §29 относно чл. 27к, ал. 1, думите "временно да спре или" се заличават.

Мотиви: не следва НКО да може спира лиценз извън предвидения за това ред в специален закон. Следва да бъдат оставени само сезирането на компетентния орган по издаване и съда.

19. В §30, чл. 29 се правят следните изменения:
а) В ал. 2 думите "но не по-малко от 20 000 000 лв" се заменят с думите "или 20 000 000 лв., която от двете суми е по-голяма"
б) В ал. 3 думите "но не по-малко от 14 000 000 лв." се заменяет с думите "или 14 000 000 лв., която от двете суми е по-голяма"

Мотиви: редакционни предложения за постигане на повече яснота на административнонаказателните разпоредби.

20. В 32 се създава т. 3:
3. Създават се ал. 7-8:
(7) При прилагане на ал. 1, компетентните органи по чл. 27е, съобразяват следните смекчаващи вината обстоятелства:
1. сериозността на нарушението и значимостта на нарушените разпоредби, като се има предвид, че за тежко нарушение се считат във всички случаи наред с другото.
а). повторни нарушения;
б). неуведомяване или липса на реакция при значителни инциденти;
в). наличие на неотстранени в разумен срок недостатъци, посочени в обвързващи указания от компетентните органи;
г). възпрепятстване на одити или дейности по мониторинг от компетентния орган след констатация на нарушение;
д). предоставяне на невярна или неточна информация във връзка с мерките за управление на риска в областта на киберсигурността или задълженията за докладване;
2. продължителността на нарушението;
3. предишни нарушения от страна на съответния субект;
4. причинени материални или нематериални вреди, включително финансови или икономически загуби, въздействия върху други услуги и брой на засегнатите потребители;
5. умисъл или небрежност от страна на извършителя на нарушението;
6. всички предприети от субекта мерки за предотвратяване или ограничаване на материалните или нематериалните вреди;
7. всяко придържане към одобрени кодекси на поведение или одобрени механизми за сертифициране;
8. съдействието, което отговорните физически или юридически лица оказват на компетентния орган;
(8) Актове за установяване на административно нарушение могат да бъдат издаване не по-рано от 6 месеца след вписване на съответния субект - нарушител в регистъра по чл. 6”

Мотиви: Макар в ЗАНН да има общи разпоредби за отчитане на смекчаващи вината обстоятелства, текстът от директивата въвежда конкретика в това кои обстоятелства са смекчаващи в конкретния контекст. Поради това е нужно текстът на директивата да бъде пренесен в закона.
С ал. 8 се предвижда период от 6 месеца, в който задължените субекти могат да приведат дейността си в съответствие с изискванията на закона, като те текат от момента на вписването им в регистъра по чл. 6, т.е. Момента на определянето им като такива, попадащи в обхвата на закона.

21. В § 33 се правят следните изменения:
а) Точка 1 се изменя така:
“1. В т. 1 думите “закона за електронното управление” се заменят с думите “Административнопроцесуалния кодекс”
б) създава се т. о1:
“о1. Точка 24 се изменя така:
24. “Онлайн място за търговия” е услуга, която чрез използване на софтуер, включително уебсайт, част от уебсайт или приложение, управлявани от търговеца или от негово име, позволява на потребителите да сключват договори от разстояние с други търговци или потребители”

Мотиви: прецизиране на дефиниции, като дефиницията на Онлайн място за търговия е в съответствие с приложимата европейска нормативна уредба

22. В §34, съдържанието на колоната “Вид субект” да се синхронизира с директивата

Мотиви: В проекта по вносител има препратки към разпоредби и определения в други закони, като това създава едновременно неяснота при тълкуването, и риск от неправилно транспониране. Следва конкретните редакции са бъдат уточнени в рамките на работна група.

23. В §35 думите “До 17 януари 2025 г.” се заменят с думите “В тримесечен срок от обнародването на този закон”

24. В §40 думите “три месеца” се заменят с думите “6 месеца”

Мотиви: прецизиране и удължаване на сроковете с оглед на забавянето в приемането на закона

25. В преходните и заключителни разпоредби се създава § 36а със следния текст:
“§ 36а. Министерският съвет приема национална стратегия за киберсигурност в срок от 9 месеца от приемането на този закон”

Мотиви: С разпоредбата се създава задължение за Министерския съвет да приеме стратегията, тъй като настоящата е изключително остаряла.

26. В преходните и заключителни разпоредби се създава § 44а

§ 44а. В Закона за защита на класифицираната информация (..) се правят следните изменения и допълнения:
1. В Приложение № 1 към чл. 25, Раздел II, т. 14 се отменя:

2. В Приложение № 1 към чл. 25, Раздел II, в т. 15 накрая се добавят думите "освен ако същите мрежи не се използват и за други нужди, като в този случай настоящата точка се прилага единствено за елементите, които обслужват предаването на класифицирана информация и превенцията на установяването на местоположение на обекти, което представлява държавна тайна":

Мотиви: Класифицирането на сведения за информационни системи и мрежи създава трудности пред тяхното опериране и поддържане, без да дава допълнително ниво на сигурност, като в същото време ограничава и конкуренцията в сферата на киберсигурността. За ограничаване на достъпа до такава информация е предвидена TLP схемата за класификация, уредена в наредбата към настоящия закон.

27. В преходните и заключителни разпоредби се създава § 44б:

§ 44б. В чл. 64 от Закона за министерството на вътрешните работи (..) се създава ал. 8: "(8) Когато разпореждането е свързано с преустановяване на достъпа до интернет адреси или до филтриране на интернет трафик, разпореждането се съгласува по реда на чл. 14, ал. 5, изречение второ от Закона за киберсигурност и се включва в доклада по чл. 14, ал. 5, изречение четвърто от Закона за киберсигурност."

Мотиви: Аналогично на мотивите за изменение на чл. 14, ал. 5 във връзка с потенциални злоупотреби с полицейски разпореждания за преустановяване на достъпа до интернет адреси.

ВНОСИТЕЛИ:

Recoverable Signature

X Божидар Божанов

Божидар Божанов

Signed by: BOZHIDAR PLAMENOV BOZHANOV

Божидар Божанов