

РЕПУБЛИКА БЪЛГАРИЯ  
НАРОДНО СЪБРАНИЕ

---

*Проект*

**ЗАКОН**

**ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА НАКАЗАТЕЛНИЯ КОДЕКС**

(Обн., ДВ, бр. 26 от 1968 г.; попр., бр. 29 от 1968 г.; изм. и доп., бр. 92 от 1969 г., бр. 26 и 27 от 1973 г., бр. 89 от 1974 г., бр. 95 от 1975 г., бр. 3 от 1977 г., бр. 54 от 1978 г., бр. 89 от 1979 г., бр. 28 от 1982 г.; попр., бр. 31 от 1982 г.; изм. и доп., бр. 44 от 1984 г., бр. 41 и 79 от 1985 г.; попр., бр. 80 от 1985 г.; изм. и доп., бр. 89 от 1986 г.; попр., бр. 90 от 1986 г.; изм. и доп., бр. 37, 91 и 99 от 1989 г., бр. 10, 31 и 81 от 1990 г., бр. 1 и 86 от 1991 г.; попр., бр. 90 от 1991 г.; изм. и доп., бр. 105 от 1991 г., бр. 54 от 1992 г., бр. 10 от 1993 г., бр. 50 от 1995 г.; Решение № 19 на Конституционния съд от 1995 г. - бр. 97 от 1995 г.; изм. и доп., бр. 102 от 1995 г., бр. 107 от 1996 г., бр. 62 и 85 от 1997 г.; Решение № 19 на Конституционния съд от 1997 г. - бр. 120 от 1997 г.; изм. и доп., бр. 83, 85, 132, 133 и 153 от 1998 г., бр. 7, 51 и 81 от 1999 г., бр. 21 и 51 от 2000 г.; Решение № 14 на Конституционния съд от 2000 г. - бр. 98 от 2000 г.; изм. и доп., бр. 41 и 101 от 2001 г., бр. 45 и 92 от 2002 г., бр. 26 и 103 от 2004 г., бр. 24, 43, 76, 86 и 88 от 2005 г., бр. 59, 75 и 102 от 2006 г., бр. 38, 57, 64, 85, 89 и 94 от 2007 г., бр. 19, 67 и 102 от 2008 г., бр. 12, 23, 27, 32, 47, 80, 93 и 102 от 2009 г., бр. 26 и 32 от 2010 г., бр. 33 и 60 от 2011 г., бр. 19, 20 и 60 от 2012 г., бр. 17, 61 и 84 от 2013 г., бр. 19, 53 и 107 от 2014 г., бр. 14, 24, 41, 74, 79 и 102 от 2015 г., бр. 32 и 47 от 2016 г.; Решение № 12 на Конституционния съд от 2016 г. - бр. 83 от 2016 г.; изм. и доп., бр. 95 от 2016 г., бр. 13, 54, 85 и 101 от 2017 г., бр. 55 от 2018 г., бр. 1, 7, 16 и 83 от 2019 г. и бр. 13, 23 и 28 от 2020 г.)

§ 1. В чл. 155б, ал. 1 думата „пет“ се заменя с „шест“.

§ 2. В чл. 155в думата „пет“ се заменя с „шест“.

§ 3. В чл. 159, ал. 3 думата „три“ се заменя с „шест“.

§ 4. В чл. 172а се правят следните изменения:

1. В ал. 1 думите „до пет години“ се заменят с „от една до шест години“, а думите „пет хиляди“ се заменят с „десет хиляди“.

2. В ал. 2 думите „пет години“ се заменят с „шест години“, а думите „пет хиляди“ се заменят с „десет хиляди“.

3. В ал. 3 думите „от една до шест години“ се заменят с „от две до осем години“, а думите „десет хиляди“ се заменят с „петнадесет хиляди“.

**§ 5.** В чл. 172б се правят следните изменения и допълнения:

1. В ал. 1 след думата „марка“ се добавя „изобретение, полезен модел“ и се поставя запетая, а думите „до пет години и с глоба до пет хиляди“ се заменят с „от една до шест години и с глоба до десет хиляди“.

2. В ал. 2 думите „от пет хиляди до осем хиляди“ се заменят с „от десет хиляди до петнадесет хиляди“.

**§ 6.** В чл. 173 се правят следните изменения и допълнения:

1. В ал. 1 думата „две“ се заменя с „три“.

2. Създава се ал. 3:

„(3) Когато деянието по ал. 1 и 2 е извършено в интернет или са причинени значителни вредни последици, наказанието е лишаване от свобода до шест години и глоба до десет хиляди лева.“

**§ 7.** В чл. 175, ал. 1 след думите „чл. 173“ се поставя запетая и се добавя „ал. 1 и 2“.

**§ 8.** В чл. 319а се правят следните изменения и допълнения:

1. В ал. 1 думите „две години“ се заменят с „шест години и с глоба до три хиляди лева“.

2. В ал. 2 думите „две години“ се заменят с „шест години“, а думите „три хиляди“ се заменят с „пет хиляди“.

3. В ал. 3 след думите „електронен подпис“ се добавя „или лични данни“, думата „три“ се заменя със „седем“, а думите „пет хиляди“ се заменят с „двадесет хиляди“.

4. В ал. 4 след думата „тайна“ се добавя „или срещу информационна система, която е част от критичната инфраструктура“ и се поставя запетая, а думите „от една до три години“ се заменят с „от четири до осем години“.

5. В ал. 5 думите „от една до осем години“ се заменят с „от пет до дванадесет години“.

**§ 9.** В чл. 319б се правят следните изменения:

1. В ал. 1 думата „две“ се заменя с „шест“, а думите „три хиляди“ се заменят с „десет хиляди“.

2. В ал. 2 думата „три“ се заменя със „седем“, а думите „пет хиляди“ се заменят с „двадесет хиляди“.

3. В ал. 3 думите „от една до три години“ се заменят с „от пет до седем години“, а думите „пет хиляди“ се заменят с „десет хиляди“.

4. В ал. 4 думите „от една до четири години“ се заменят с „от пет до осем години“, а думите „шест хиляди“ се заменят с „двадесет хиляди“.

5. В ал. 5 думите „от пет до осем години“ се заменят с „от девет до дванадесет години“, а думите „десет хиляди“ се заменят с „тридесет хиляди“.

**§ 10.** В чл. 319в се правят следните изменения:

1. В ал. 1 думите „три години“ се заменят със „седем години“, а думите „три хиляди“ се заменят с „пет хиляди“.

2. В ал. 2 думите „от една до три години“ се заменят с „от пет до седем години“, а думите „пет хиляди“ се заменят със „седем хиляди“.

**§ 11.** В чл. 319г се правят следните изменения и допълнения:

1. В ал. 1 думите „три години“ се заменят със „седем години“, а думите „три хиляди“ се заменят с „пет хиляди“.

2. В ал. 3 думата „пет“ се заменя с „девет“, а думите „три хиляди“ се заменят с „двадесет хиляди“.

3. Създава се ал. 4:

„(4) Ако деянието по ал. 1 и 2 е извършено срещу информационна система или компютърна мрежа, която е част от критичната инфраструктура, наказанието е лишаване от свобода от пет до дванадесет години и глоба до двадесет хиляди лева.“

**§ 12.** В чл. 319д се правят следните изменения:

1. В ал. 1 думата „две“ се заменя с „шест“.

2. В ал. 2 думите „до три години“ се заменят с „от четири до седем години“.

3. В ал. 3 думата „пет“ се заменя с „девет“.

**§ 13.** В чл. 319е след думите „се наказва с“ се добавя „лишаване от свобода до шест години и“.

**ЗАКЛЮЧИТЕЛНА РАЗПОРЕДБА**

**§ 14.** В Закона за електронната търговия (обн., ДВ, бр. 51 от 2006 г.; изм. и доп., бр. 105 от 2006 г., бр. 41 от 2007 г., бр. 82 от 2009 г., бр. 77 и 105 от 2011 г., бр. 57 от 2015 г., бр. 94 от 2018 г. и бр. 17 от 2019 г.), в чл. 16, ал. 3 се създава изречение второ:

„Доставчикът е длъжен да съхранява и предоставя информацията в срок от шест месеца след прекратяване на договора му с получателя на услугата.“

Законът е приет от 44-ото Народно събрание на ..... 2020 г. и е подпечатан с официалния печат на Народното събрание.

**ПРЕДСЕДАТЕЛ НА  
НАРОДНОТО СЪБРАНИЕ:**

**(Цвета Караянчева)**

## МОТИВИ

### КЪМ ПРОЕКТА НА ЗАКОН ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА НАКАЗАТЕЛНИЯ КОДЕКС

Киберпрестъпността е обществено явление, което не признава граници, възползва се от постоянно разрастващата се глобализация, от новите технологии, от регионалните и националните кризи в страните — било то икономически, политически или военни. Ежедневно ставаме свидетели на мащабни и разнородни кибератаки, нанасящи огромни щети на компании и интернет потребители от цял свят, като същите са факт и в страната ни. Нещо повече, киберпрестъпността и употребата на интернет пространството успешно и ефективно благоприятства и всяка една останала престъпна дейност на национално и транснационално ниво, която нанася огромни щети на бюджета.

В последното десетилетие е налице рязко и масово нахлуване на технологиите и интернет пространството в ежедневието на обществото ни като част от неговото развитие. С това във времето все повече се разширява и възможният обект на престъпления от подобен тип посегателства - засягат се както икономическите отношения (чл. 216, ал. 3-6, чл. 212а, чл. 246, ал. 3, чл. 319а, чл. 319б, чл. 319в от НК), така и неприкосновеността на кореспонденцията ни (чл. 171 и чл. 319д от НК), правата, защитаващи интелектуалната собственост, и други. Към днешна дата обект на компютърните атаки могат да бъдат както държавата, така и бизнесът и гражданите.

Горепосоченото се потвърждава и от статистика на Главна дирекция „Борба с организираната престъпност“ към Министерството на вътрешните работи за постъпили сигнали от жертви на компютърни и компютърно свързани престъпления през последните 5 години, чиито показатели са следните:

Таблица 1

Година	Постъпили жалби и сигнали от жертви на киберпрестъпления	Взето отношение по постъпилите жалби и сигнали, съдържащи съставомерност по Наказателния кодекс
2015	57	39
2016	757	543
2017	1308	971
2018	2384	1660
2019	2822	2049
Общо	7328	5262

По данни от Годишния отчет за електронното управление за 2018-2019 г. на Държавна агенция „Електронно управление“ в периода август 2018 г. - юли 2019 г. Националният екип за реагиране при инциденти с компютърната сигурност към Държавна агенция „Електронно управление“ констатира непрекъснато усложняване на обстановката в киберсигурността на страната.

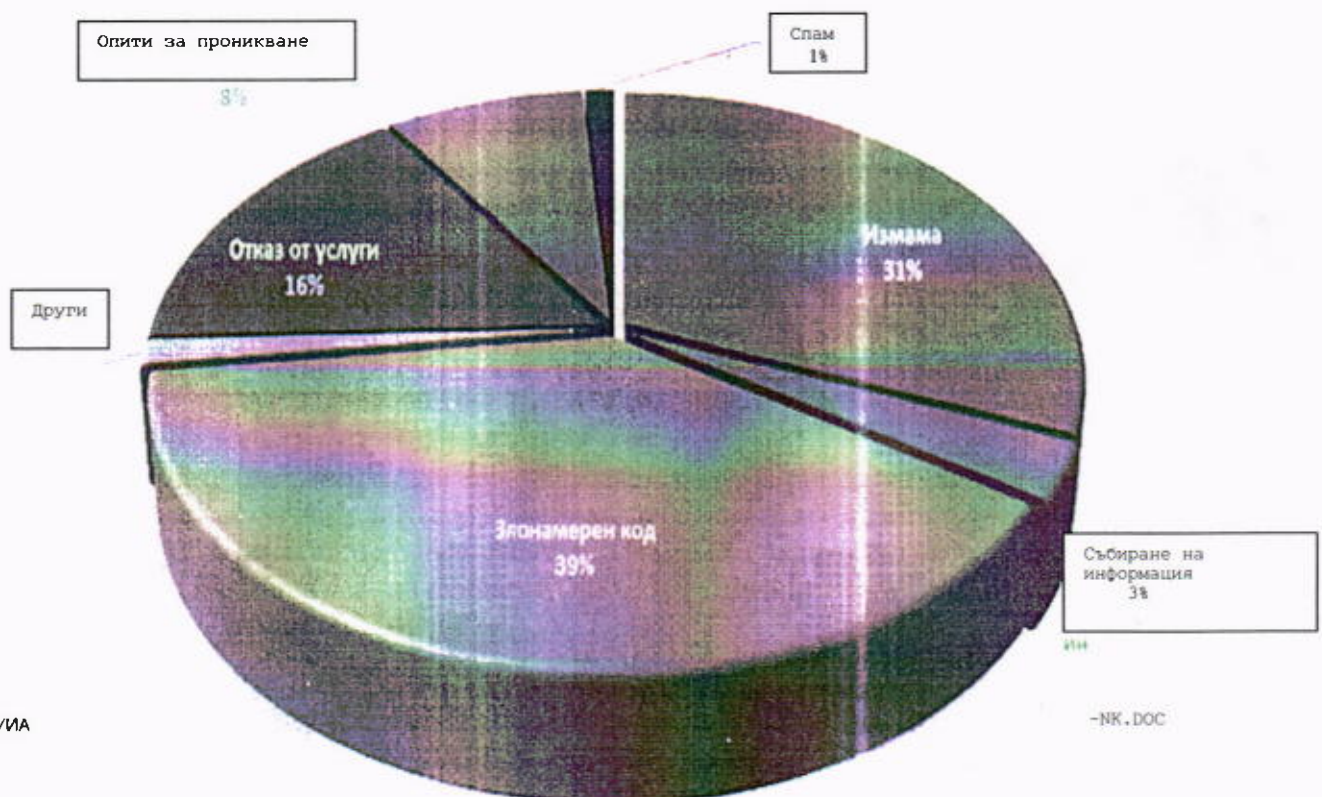
В таблицата по-долу е показана статистика за отчетния период, свързана с регистрирани инциденти в централните и териториалните администрации, при които мрежовата и информационната сигурност е с висок и среден приоритет:

Таблица 2

№	Тип на инцидента	Брой засегнати администрации
1	DDoS (разпределен отказ от услуга)	13
2	Ransomware (криптиращ вирус)	4
3	Intrusion Attempts (общо проникване)	1
4	Unauthorised Access to Information (неоторизиран достъп до информация)	9
5	Кражба на лични данни	1
6	Уязвимост	2
7	Phishing (измамнически сайт)	3
8	SQL injection	2

## ВИДОВЕ РЕГИСТРИРАНИ ИНЦИДЕНТИ

Фиг. 1 Обем на базите данни



Хакерски групи продължават да се насочват към субекти в държавите - членки на ЕС, в т.ч. и България, с цел придобиване на чувствителна информация. Най-значимите атаки на тези групи са насочени към мрежови устройства, като рутери, комутатори, защитни стени, мрежово базирани системи за откриване на прониквания (Intrusion Detection System), разположени в мрежите предимно на правителствени и частни организации, ръководители на обекти от критичната инфраструктура и доставчици на достъп до интернет (ISP), които поддържат тези сектори.

Националният екип за реагиране при инциденти с компютърната сигурност ежесечно в изпълнение на проактивните си действия изпраща бюлетин до служителите в публичната администрация, отговарящи за мрежовата и информационната сигурност. Бюлетинът съдържа статистика на инцидентите за предходния месец, информация и препоръки за добри практики.

В допълнение на това в годишния си доклад за 2019 г. Центърът по киберсигурност към Европол също отчита, че киберпрестъпленията стават все по-дръзки, а фокусът им се измества към по-големи и по-печеливши цели. В тази връзка Центърът по киберсигурност препоръчва държавите членки да прилагат законодателство, което да отговаря на динамиката, с която се развиват технологиите.

В доклада се посочва също така тревожна статистика по отношение на т.н. компютърен саботаж в частния сектор, а именно компютърните престъпления, при които не само неправомерно се достъпва дадена информационна система, но и данните в нея се увреждат или унищожават с цел затрудняване работата на съответното юридическо лице. Това води до нарастващ страх в частния сектор. Статистиката през първите 6 месеца на 2019 г. показва, че кибератаките, предназначени да причиняват щети, са се удвоили, като 50% от атакуваните фирми са били в производствения сектор. Това принуждава представителите на частния сектор да правят вложения в защитени резервни копия на данните, тъй като иначе биха загубили трайно своите данни.

Също така на 14 октомври 2019 г. в Министерството на правосъдието постъпи официално уведомително писмо на Европейската комисия (ОУП) № С (2019) 6272 по Процедура за нарушение № 2019/2240 относно неизпълнение на задълженията на Република България във връзка с чл. 9, пар. 4, буква „б“ и буква „в“ от Директива 2013/40/ЕС относно атаките срещу информационните системи. Според констатациите на Европейската комисия при транспонирането на Директива 2013/40/ЕС България не се е съобразила с изискуемия максимален праг на наказанието лишаване от

свобода, предвиден в случаите, посочени в чл. 9, пар. 4 от Директивата, който следва да бъде не по-малък от пет години. Този праг се предвижда, когато деянията по чл. 4 и 5 от Директивата са причинили сериозни вреди или са извършени срещу информационна система, която е част от критична инфраструктура.

Особено важно за нормалното функциониране на държавата е осигуряването на безпроблемната работа както на държавния апарат, така и на обектите от стратегическо значение в различните структуроопределящи сектори, като земеделието, транспорта, енергетиката, здравеопазването и други, които са част от т.н. критична инфраструктура. Нарушаването на нормалното ѝ функциониране може да доведе до сериозни финансови загуби, до заплахата за националната сигурност на страната, а също и до нарушаване на нормалното снабдяване на обществото с жизненоважни услуги и/или продукти. През 2019 г. в европейски план се наблюдава разширяване на обхвата на представляващите критична инфраструктура обекти в европейските държави в резултат на повишената бдителност на националните компетентни органи и на увеличаващия се брой кибератаки.

Сред предлаганите изменения се включва и актуализиране на нормативната уредба за противодействие спрямо компютърно свързаните престъпления по чл. 172а, 172б и 173 от НК срещу интелектуалната и индустриалната собственост, както и онлайн детската сексуална експлоатация по чл. 155б, 155в и 159, ал. 3 от НК с оглед на постигане на съответствие между обществената опасност на тези престъпления и предвидените от закона наказания. Тези престъпления следва да се възприемат за деяния с висока степен на обществена опасност, не само предвид правата и интересите на отделния автор, които засягат, а и с нанасянето на финансови загуби в особено големи размери, което се отразява на приходите в държавния бюджет. Сексуалната експлоатация на децата се увеличава и разпространява посредством използването на новите технологии и интернет.

Също така основен критерий за оценка ефективността на противодействието на една държава срещу нарушаването на авторските права е ежегодният "Watch List" (Списък за наблюдение) на правителството на САЩ, преглед по Раздел „Специален 301“. В резултат на предприетите досега от правителството на Република България мерки за противодействие на нарушаването на авторските права България беше извадена от последните два доклада за 2017 г. и 2018 г. от Списък „Специален 301“. Преди това страната ни е била включвана в списъка последователно пет поредни години.



Наред с другите предприемани мерки са необходими и законодателни, тъй като при липса на такива, страната ни е заплашена да попадне отново в Списък „Специален 301“ за доклада през 2019 г., който ще бъде публикуван през 2020 г.

Във връзка с изложеното се налага актуализиране на действащата нормативна уредба на компютърните и компютърно свързаните престъпления в Особената част на Наказателния кодекс - глава втора, раздел VIII, глава трета, раздел VII и глава девета „а“, с цел осигуряване на по-адекватна защита на държавата, бизнеса и гражданите от неправомерни деяния, засягащи техните основни права.

В последните години се наблюдава тенденция на дигитализиране и автоматизиране на все повече услуги и процеси, които са свързани както със стопанския живот, така и с ежедневните дейности на гражданите. Съвременните технологии позволяват сключване на сделки, банкови трансфери, съхранение на и достъп до лични данни и друга чувствителна информация онлайн. Блокчейн като иновативна технология за верифициране навлиза във все по-широк кръг обществени отношения. На практика няма дейност, която да се осъществява без електронен обмен на дигитална информация. Компютрите се превръщат в средство за извършване на повечето престъпления, инкриминирани в Наказателния кодекс. Увеличаването на възможностите на компютърните технологии води и до увеличаване на опасността от засягане на правата на гражданите. По тази причина все по-широк кръг обществени отношения са засягани от компютърни престъпления или от престъпления, извършени чрез използване на компютърни мрежи или системи. От друга страна, се наблюдава тенденция към увеличаване на тежестта на засягане на обществените отношения от компютърни и компютърно свързани престъпления. Изграждането на автоматизирани информационни бази данни прави възможно засягането на много широк кръг лица, създавайки условия за последващо извършване на множество други престъпления, засягащи правата на широк кръг лица.

С оглед на гореизложените съображения предлагам Народното събрание да разгледа и приеме проекта на Закон за изменение и допълнение на Наказателния кодекс.

**МИНИСТЪР-ПРЕДСЕДАТЕЛ:**

**(Бойко Борисов)**