Приложение № 1
към чл. 16 от Наредбата за обхвата и методологията за извършване на оценка на въздействието

Формуляр за частична предварителна оценка на въздействието* (Приложете към формуляра допълнителна информация/документи)	
Институция: **Министерство на правосъдието**	**Нормативен акт:** Проект на Закон за изменение и допълнение на Наказателния кодекс
За включване в законодателната програма на Министерския съвет за периода: **30.06.2020 г. – 31.12.2020 г.**	**Дата: 03.06.2020 г.**
Контакт за въпроси: Александър Стефанов, държавен експерт в дирекция „Съвет по законодателство“ на Министерство на правосъдието, ел. поща: Al_Stefanov@justice.government.bg.; Емилия Александрова, държавен експерт в дирекция „Съвет по законодателство“ на Министерство на правосъдието, ел. поща: Em_Aleksandrova@justice.government.bg.	**Телефон:** 02 / 9237 344 **Телефон:** 02 / 9237 463

1. Дефиниране на проблема:

1.1. Кратко опишете проблема и причините за неговото възникване. Посочете аргументите, които обосновават нормативната промяна.

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, което 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. 319 б и чл. 319в НК), така и неприкосновеността на кореспонденцията ни (чл. 171 и чл. 319д НК), правата, защитаващи интелектуалната собственост, и други. Към днешната дата обект на компютърните престъпления могат да бъдат както държавата, така и бизнесът и гражданите.

Горепосоченото се потвърждава и от статистиката 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 имащи [illegible]
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 Държавната агенция „Електронно управление“ в периода август 2018 г. - юли 2019 г. Националният екип за реагиране при инциденти в компютърната сигурност към Държавната агенция „Електронно управление“ констатира непрекъснато усложняване на обстановката в киберсигурността на страната.

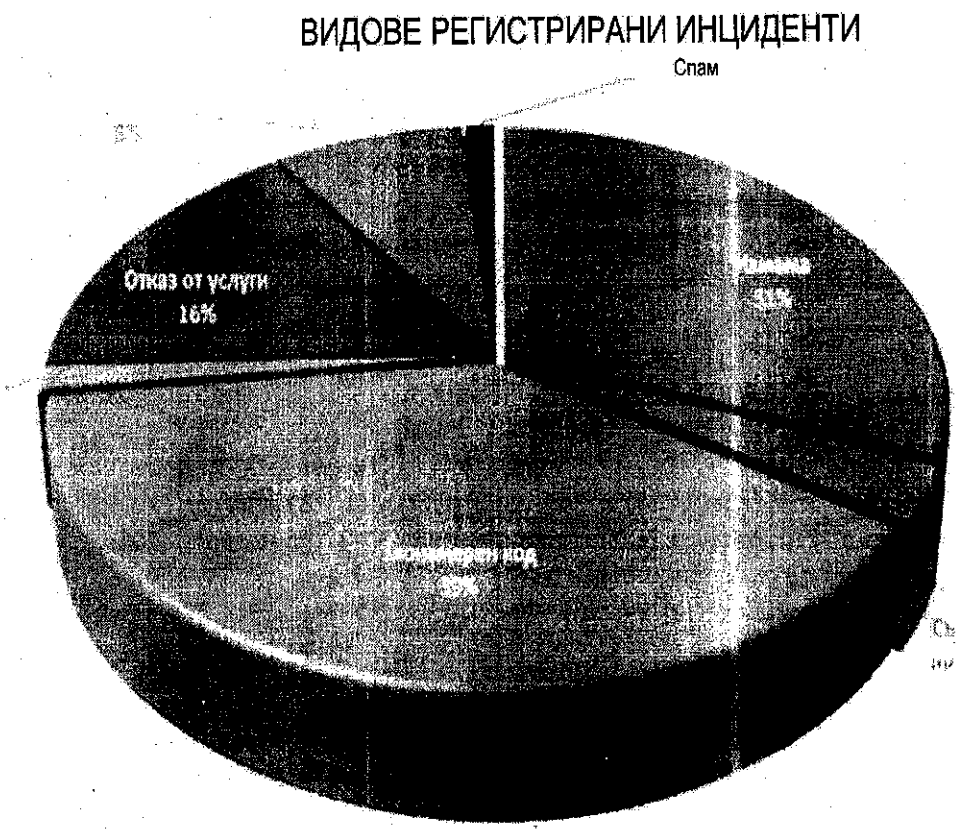
В таблицата по-долу е показана статистика за отчетния период, свързана с регистрирани инциденти в централните и териториалните администрации е мрежовата и информационната сигурност с висок и среден приоритет:

Таблица 2

	Тип на инцидента	*Брой засегнати администрации*
	DDoS (разпределен отказ от услуга)	*13*
	Ransomware (криптиращ вирус)	*4*
	Instrusion Attempts (общо проникване)	*1*
	Unauthorised Access to information (неоторизаран достъп до информация)	*9*
	Кражба на лични данни	*1*
	Уязвимост	*2*
	Phishing (измамнически сайт)	*3*
	SQL injection	*2*

По данни от статистиката, която се води от екипа за нарушения в и от българското интернет пространство, са регистрирани 2 851 сигнала, което е с 34% увеличение спрямо предходния период. От тях като инциденти, съгласно таксономията на Европейската агенция за киберсигурност - ENISA, са регистрирани 2 030, което е увеличение с 33%. Наблюдава се рязко увеличаване на броя засегнати IP адреси в българското адресно пространство - над 6,5 пъти.

Данните от статистиката също показват, че рязко нараства относителният дял на инцидентите със значително увреждащо въздействие в мрежовата и информационната сигурност с висока степен на опасност. Най-голям е процентът на регистрираните инциденти, дължащи се на злонамерен код (malware), следвани от инцидентите, дължащи се на измама (phishing).



Фиг. 1 Обем на базите данни

Хакерските 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, комуникатори, защитни стени, мрежово базирани системи за откриване на проникванията (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 ежемесечно в изпълнение на проактивните си действия изпраща бюлетин до служителите в публичната администрация, отговарящи за мрежовата и информационна 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 една от мерките за справяне на държавите членки да бъде прилагане на закон, който трябва да бъде еднакво дързък, за да отговори на предизвикателството, и в тази връзка законодателството на държавите членки да еволюира съобразно постоянно променящите се и развиващи се технологии.

В доклада се посочва също така тревожна статистика по отношение на т.нар. 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 у 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 частния сектор да прави 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. Деянията по чл. 4 от Директивата (незаконна намеса в системи) са въведени в чл. 319г от Наказателния кодекс. В разпоредбата на чл. 319г не е предвидена изрична уредба на случаите, когато намесата е насочена срещу информационна система, която е част от критична инфраструктура, което се отклонява от изискванията на чл. чл. 9, пар. 4 от Директивата. В тези случаи максималният срок на лишаването от свобода следва да бъде най-малко пет години.

С предложения проект на Закон за изменение и допълнение на Наказателния кодекс (ЗИД на НК) се цели повишаването на информационната сигурност чрез въвеждането на по-висока степен на наказателноправна защита срещу извършването на компютърни престъпления, която да съответства на тяхната реална обществена опасност и да способства за ефективното разследване на подобен вид деяния.

1.2. Опишете какви са проблемите в прилагането на съществуващото законодателство или възникналите обстоятелства, които налагат приемането на ново законодателство. Посочете възможно ли е проблемът да се реши в рамките на съществуващото законодателство чрез промяна в организацията на работа и/или чрез въвеждане на нови технологични възможности (например съвместни инспекции между няколко органа и др.).

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. Това е т. ар. критична инфраструктура. Нарушаването на нормалното ѝ функциониране може да доведе освен до сериозни финансови загуби, до заплаха за националната сигурност на страната, а също и до нарушаване на нормалното снабдяване на обществото с жизнено важни услуги и/или продукти. През 2019 г. в европейски план се наблюдава разширяване на обхвата на представляващите критична инфраструктура обекти от разследващите органи в европейските държави, като дължащо се както на повишената бдителност на националните компетентни органи, така и на увеличаващия се брой кибератаки.

Същевременно по линия противодействие този вид престъпления, извършени в и чрез дигитална среда, са налице трудности при документиране на престъпната дейност и установяване на извършителя, произтичащи от настоящата законодателна уредба и

по-конкретно от Закона за електронните съобщения (ЗЕС) и Наказателния кодекс (НК). Съгласно чл. 251б, ал. 2 от ЗЕС компютърно-информационни данни могат да се изискват по съответния ред, само когато са свързани с извършено тежко умишлено престъпление - тоест предвидено е наказание над 5 години лишаване от свобода.

Невъзможността, поради съществуващата регламентация в ЗЕС, да се водят ефективни проверки и разследвания от полицейските органи и органите на досъдебното производство обхваща и почти всички текстове на глава девета „а"; глава втора, раздел VIII и глава трета, раздел VII от особената част на НК. По-конкретно деяния по чл. 319д от НК, при които лице създава, набавя за себе си или за другиго, внася или по друг начин разпространява компютърни програми, пароли, кодове или други подобни данни за достъп до информационна система или част от нея с цел да се извърши престъпление по чл. 171, ал. 3, чл. 319а, чл. 319б, чл. 319в или чл. 319г, са извън обхвата на настоящата регламентация по ЗЕС, което прави практическото им разследване невъзможно. В същото време това е и единственият начин за събиране на дигитални следи, от които може да се достигне до извършителя на престъплението. Подобна е правната уредба и на деянията по чл. 319г от НК, касаещи въвеждането на компютърен вирус в информационна система или компютърна мрежа, както и въвеждането на друга компютърна програма, която е предназначена за нарушаване на дейността на информационна система или компютърна мрежа или за узнаване, заличаване, изтриване, изменение или копиране на компютърни данни без разрешение, когато такова се изисква. Противоправни деяния, изразяващи се в неправомерно осъществен достъп до информационна система или части от нея, при които не са настъпили тежки последици, както и при достъп до или промяна на компютърни данни в информационна система, когато това не е свързано е дейността на организирана престъпна група или достъпът не касае критична инфраструктура, също на практика не могат да бъдат ефективно разследвани и пресичани.

Престъпленията срещу интелектуалната собственост, авторското право и сродните му права (глава трета, раздел VII от особената част на НК) са деяния с висока степен на обществена опасност, не само предвид правата и интересите на авторите, които засягат, а и с нанасянето на финансови загуби в особено големи размери, което се отразява на приходите в държавния бюджет. Тяхното разследване също е невъзможно да бъде извършено без изискване на т.нар. „трафични данни".

Същевременно децата, като едни от най-малките и най-активни потребители на интернет пространството, са ежедневно изложени на порнографско съдържание, което още от ранна възраст провокира деструктивно действие върху оформянето на личността им. Нещо повече, малолетни и непълнолетни ежедневно стават жертви на сексуални набези от страна на лица, имащи такъв тип сексуално поведение. В тази връзка са необходими спешни промени и на съставите на престъпления в глава втора, раздел VIII от особената част на НК - „Разврат".

От изложеното по-горе става ясно, че освен наличието на усложнена кибер обстановка както в Република България, така и в Европейския съюз, е налице необходимост и от осигуряване на възможност на правоохранителните органи пълноценно да могат да извършват разследвания на компютърните престъпления, извършвани на територията на страната.

Така формулирана, нормата на чл. 251б, ал 2 от ЗЕС не позволява придобиването по единствения възможен начин на значима за разкриването и разследването на тези престъпления информация, при почти всички състави на визираните по-горе престъпления:

- за същинските компютърни престъпления от Глава девета „а" от НК;
- за компютърно свързаните престъпления в Глава втора, раздел VIII от НК - онлайн детска сексуална експлоатация и Глава трета, раздел VII от НК - интелектуална, индустриална собственост и авторско право.

Съставите на горепосочените престъпления предвиждат наказания лишаване от свобода по-малко от 5 години или до 5 години. От друга страна, за ефективното им наказателно преследване е необходимо да бъде получена информация по чл. 251б от ЗЕС (трафични данни). Съгласно ал. 2 на същия, такива данни се съхраняват за нуждите на националната сигурност и за предотвратяване, разкриване и разследване на тежки престъпления. В този смисъл е и решение на Конституционния съд № 2 от 12 март 2015 г. по конституционно дело № 8 от 2014 г. Със същото съдът обявява за противоконституционни актуалните към 2014 г. текстове на ЗЕС, като намира, че същите не удовлетворяват установените европейски стандарти за гарантиране на конституционно закрепените основни права на гражданите. Решението на Конституционния съд е в пряка връзка с Решение на Съда на ЕС от 8.04.2014 г., разширен състав, по съединени дела С-293/12 и С-594/12, (по-известно като *Digital rights Ireland*), с което транспонираната в ЗЕС Директива 2006/24/ЕО е обявена за невалидна поради несъответствието ѝ с разпоредбите на чл. 7, чл. 8 и чл. 52, § 1 от Хартата на основните права на Европейския съюз. Съдебната практика на Съда на ЕС относно съхранението на данни е доразвита с Решение на Съда от 21.12.2016 г. по съединени дела С 203/15 и С 698/15 (известно и като *Tele 2 & Watson*). В същото Съдът на ЕС потвърждава, че събирането на трафични данни е мярка, чийто характер предпоставя сериозно ограничаване на правото на личен и семеен живот и на правото на защита на личните данни (защитени в чл. 7 и чл. 8 от Хартата на основните права на ЕС), поради което достъп до трафични данни е възможен само за целите на превенция, разследване и наказателно преследване на тежки престъпления. Така практиката на Съда на ЕС прави невъзможно използването на трафични данни при извършени престъпления, които не са тежки по смисъла на националното законодателство на всяка държава членка.

В разпоредбата на чл. 319г следва да се предвиди изрична уредба на случаите, когато намесата е насочена срещу информационна система, която е част от критична инфраструктура в съответствие с изискванията на чл. чл. 9, пар. 4 от Директивата. В тези случаи максималният срок на лишаването от свобода следва да бъде най-малко пет години.

Въвеждането на по-висока степен на наказателноправна защита срещу извършването на компютърни престъпления, която да съответства на тяхната реална обществена опасност и да способства за ефективното разследване на подобен вид деяния, не може да се реши в рамките на съществуващото законодателство чрез промяна в организацията на работа и/или чрез въвеждане на нови технологични възможности.

1.3. Посочете дали са извършени последващи оценки на нормативния акт, или анализи за изпълнението на политиката и какви са резултатите от тях?

Не е правена последваща оценка на въздействието на НК.

2. Цели: *Посочете целите, които си поставя нормативната промяна, по конкретен и измерим начин и график, ако е приложимо, за тяхното постигане. Съответстват ли целите на действащата стратегическа рамка?*

Целите, които си поставя законопроекта, е повишаването на информационната сигурност чрез въвеждането на по-висока степен на наказателноправна защита срещу извършването на компютърни престъпления, която да съответства на тяхната реална обществена опасност и да способства за ефективното разследване на подобен вид деяния.

От описаните по-горе проблеми става ясно, че се налага актуализиране на действащата нормативна уредба на компютърните и компютърно свързаните

престъпления в Наказателния кодекс, във връзка с което и с оглед осигуряване на по-адекватна защита на държавата, бизнеса и гражданите от неправомерни деяния, засягащи техните основни права, предлагаме в глава втора, раздел VIII, глава трета, раздел VII и глава девета „а" от НК увеличаване на размера на наказанията и включване на квалифицирани състави на престъпления за компютърни и компютърно свързани престъпления с оглед постигане на съответствие между обществената опасност на тези престъпления и предвидените от закона наказания.

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 НК. Увеличаването на възможностите на компютърните технологии води и до увеличаване на опасностите и възможностите за 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.

Във връзка с постъпило официално уведомително писмо на Европейската комисия (ОУП) № С (2019) 6272 по процедура за нарушение № 2019/2240 относно пълното въвеждане на изискванията на чл. 9, пар. 4, буква „б" и буква „в" от Директива 2013/40/ЕС относно атаките срещу информационните системи, като в разпоредбата на чл. 319г НК се предвиди изрична уредба на случаите, когато намесата е насочена срещу информационна система, която е част от критична инфраструктура в съответствие с изискванията на чл. 9, пар. 4 от Директивата. В тези случаи максималният срок на лишаването от свобода следва да бъде най-малко пет години.

3. Идентифициране на заинтересованите страни: *Посочете всички потенциални засегнати и заинтересовани страни, върху които предложението ще окаже пряко или косвено въздействие (бизнес в дадена област/всички предприемачи, неправителствени организации, граждани/техни представители, държавни органи, др.)*

Държавните органи и институции във връзка с работата с електронни документи;

Държавните и административните органи във връзка с предоставянето на административни услуги по електронен път;

Държавна агенция „Електронно управление";

Службите за сигурност и обществен ред;

Стратегическите обекти и на обектите и системите от критичната инфраструктура;

Органите на местното самоуправление и местната администрация;

Физическите или юридическите лица, доставчици на интернет или предоставящи услуги на информационното общество;

Физическите и юридически лица, получатели на електронни административни услуги или ползватели на интернет;

Търговците - физически и юридически лица по смисъла на чл. 1 от Търговския закон;

Носителите на авторски и сродни права.

С оглед на спецификата на регулираните с проекта на нормативен акт обществени отношения в областта на противодействието на престъпленията свързани с киберпрестъпленията и интернет, както и нарушаването на авторските и сродни права, не е възможно да се посочи точен брой на потенциалните страни.

4. Варианти на действие: *Идентифицирайте основните регулаторни и нерегулаторни възможни варианти на действие от страна на държавата, включително варианта „Без действие".*

Вариантите са следните:

Вариант 0 „Без действие" :

Неприемане на проекта на ЗИД на НК.

При този вариант няма да бъдат предприети мерки за по-добра защита от хакерски атаки и инциденти, които продължават да се насочват към субекти в държавите членки на ЕС, в т.ч. и България, с цел придобиване на чувствителна информация.

Няма да бъде налице правна уредба, насочена за предотвратяване на атаки и намесата в мрежови устройства като рутери, комуникатори, защитни стени, мрежово базирани системи за откриване на проникванията (Instrusion Detection Sistem), 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.

Няма да бъдат въведени в българското законодателство изцяло изискванията на чл. 9, пар. 4, буква „б" и буква „в" от Директива 2013/40/ЕС относно атаките срещу информационните системи, като в разпоредбата на чл. 319г НК няма да се предвиди изрична уредба на случаите, когато намесата е насочена срещу информационна система, която е част от критична инфраструктура, което се отклонява от изискванията на чл. 9, пар. 4 от Директивата. По този начин няма да бъде изпълнено задължението на Република България по процедура за нарушение № 2019/2240 във връзка с официално уведомително писмо на Европейската комисия (ОУП) № С (2019) 6272.

Няма да бъде изпълнена мярката, препоръчана от Центъра по киберсигурност към Европол в държавите членки да бъде прилаган закон, който трябва да бъде еднакво дързък, за да отговори на предизвикателството и в тази връзка законодателството на държавите членки да еволюира съобразно постоянно променящите се и развиващи се технологии.

Няма да са налице законови основания за по-адекватно противодействие 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. 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 частният сектор да прави вложения в защитени резервни копия на данните, тъй като иначе биха загубили трайно своите данни.

С неприемането на законопроекта няма да се допринесе за повишаването на информационната сигурност чрез въвеждането на по-висока степен на наказателноправна защита срещу извършването на компютърни престъпления, която да съответства на тяхната реална обществена опасност и да способства за ефективното разследване на подобен вид деяния.

Вариант 1 Приемане на проекта на ЗИД на НК:

С приемането на законопроекта ще бъдат предприети мерки за по-добра защита от хакерски атаки и инциденти, насочени към субекти в държавите членки на ЕС, в т.ч. и България, с цел придобиване на чувствителна информация.

Ще се актуализира правната уредба необходима за предотвратяване на атаки и намесата в мрежови устройства като рутери, комуникатори, защитни стени, мрежово базирани системи за откриване на проникванията (Instrusion Detection Sistem), 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.

Ще бъдат въведени в българското законодателство изцяло изискванията на чл. 9, пар. 4, буква „б“ и буква „в“ от Директива 2013/40/ЕС относно атаките срещу информационните системи. В разпоредбата на чл. 319г НК ще се предвиди изрична уредба на случаите, когато намесата е насочена срещу информационна система, която е част от критична инфраструктура, което ще бъде в съответствие с изискванията на чл. 9, пар. 4 от Директивата. По този начин ще бъде изпълнено задължението на Република България по процедура за нарушение № 2019/2240 във връзка с официално уведомително писмо на Европейската комисия (ОУП) № С (2019) 6272.

Ще бъде изпълнена мярката, препоръчана от Центъра по киберсигурност към Европол в държавите членки да бъде прилаган закон, който трябва да бъде еднакво дързък, за да отговори на предизвикателството и в тази връзка законодателството на държавите членки да еволюира съобразно постоянно променящите се и развиващи се технологии.

Ще са налице законови основания за по-адекватно противодействие 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. 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 частният сектор да прави вложения в защитени резервни копия на данните, тъй като иначе биха загубили трайно своите данни.

Приемането на законопроекта ще допринесе за повишаването на информационната сигурност чрез въвеждането на по-висока степен на наказателноправна защита срещу извършването на компютърни престъпления, която да съответства на тяхната реална

обществена опасност и да способства за ефективното разследване на подобен вид деяния.

Вариант 2: Предприемане на организационни и други мерки без нормативни промени:

Предприемането на организационни и други мерки без нормативни промени не е достатъчно и нормативно допустимо. В чл. 11, ал. 3 от Закона за нормативните актове изрично е регламентирано, че нормативните актове се отменят, изменят или допълват с изрична разпоредба на новия, изменящия или допълващия акт.

5. Негативни въздействия: *Опишете качествено (при възможност – и количествено) всички значителни потенциални икономически, социални, екологични и други негативни въздействия за всеки един от вариантите, в т.ч. разходи (негативни въздействия) за идентифицираните заинтересовани страни в резултат на предприемане на действията. Пояснете кои разходи (негативни въздействия) се очаква да бъдат второстепенни и кои да са значителни.*

Вариант 0 „Без действие“: При непредприемане на действия и неприемане на проекта няма да бъдат предприети мерки за по-добра защита от хакерски атаки и инциденти, които продължават да се насочват към субекти в държавите членки на ЕС, в т.ч. и България, с цел придобиване на чувствителна информация.

Няма да бъде налице правна уредба, насочена за предотвратяване на атаки и намесата в мрежови устройства като рутери, комуникатори, защитни стени, мрежово базирани системи за откриване на проникванията (Instrusion Detection Sistem), 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.

Няма да бъдат въведени в българското законодателство изцяло изискванията на чл. 9, пар. 4, буква „б“ и буква „в“ от Директива 2013/40/ЕС относно атаките срещу информационните системи, като в разпоредбата на чл. 319г НК няма да се предвиди изрична уредба на случаите, когато намесата е насочена срещу информационна система, която е част от критична инфраструктура, което се отклонява от изискванията на чл. 9, пар. 4 от Директивата. По този начин няма да бъде изпълнено задължението на Република България по процедура за нарушение № 2019/2240 във връзка с официално уведомително писмо на Европейската комисия (ОУП) № С (2019) 6272.

Няма да бъде изпълнена мярката, препоръчана от Центъра по киберсигурност към Европол в държавите членки да бъде прилаган закон, който трябва да бъде еднакво дързък, за да отговори на предизвикателството и в тази връзка законодателството на държавите членки да еволюира съобразно постоянно променящите се и развиващи се технологии.

Няма да са налице законови основания за по-адекватно противодействие 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. 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 частният сектор да прави вложения в защитени резервни копия на данните, тъй като иначе биха загубили трайно своите данни.

С неприемането на законопроекта няма да се допринесе за повишаването на

информационната сигурност чрез въвеждането на по-висока степен на наказателноправна защита срещу извършването на компютърни престъпления, която да съответства на тяхната реална обществена опасност и да способства за ефективното разследване на подобен вид деяния.

Посочените негативни въздействия засягат всички заинтересовани страни.

Вариант 1: С приемането на законопроекта ще бъдат предприети мерки за по-добра защита от хакерски атаки и инциденти, насочени към субекти в държавите членки на ЕС, в т.ч. и България, с цел придобиване на чувствителна информация.

Ще се актуализира правната уредба, необходима за предотвратяване на атаки и намесата в мрежови устройства като рутери, комуникатори, защитни стени, мрежово базирани системи за откриване на проникванията (Instrusion Detection Sistem), 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.

Ще бъдат въведени в българското законодателство изцяло изискванията на чл. 9, пар. 4, буква „б“ и буква „в“ от Директива 2013/40/ЕС относно атаките срещу информационните системи. В разпоредбата на чл. 319г НК ще се предвиди изрична уредба на случаите, когато намесата е насочена срещу информационна система, която е част от критична инфраструктура, което ще бъде в съответствие с изискванията на чл. 9, пар. 4 от Директивата. По този начин ще бъде изпълнено задължението на Република България по процедура за нарушение № 2019/2240 във връзка с официално уведомително писмо на Европейската комисия (ОУП) № С (2019) 6272.

Ще бъде изпълнена мярката, препоръчана от Центъра по киберсигурност към Европол в държавите членки да бъде прилаган закон, който трябва да бъде еднакво дързък, за да отговори на предизвикателството и в тази връзка законодателството на държавите членки да еволюира съобразно постоянно променящите се и развиващи се технологии.

Ще са налице законови основания за по-адекватно противодействие 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. 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 частният сектор да прави вложения в защитени резервни копия на данните, тъй като иначе биха загубили трайно своите данни.

Приемането на законопроекта ще допринесе за повишаването на информационната сигурност чрез въвеждането на по-висока степен на наказателноправна защита срещу извършването на компютърни престъпления, която да съответства на тяхната реална обществена опасност и да способства за ефективното разследване на подобен вид деяния.

При този вариант не са идентифицирани негативни въздействия.

Вариант 2 „Предприемане на организационни и други мерки без нормативни промени“: Изисква се приемане на нормативни промени в НК. Не е възможно предприемането само на организационни и други мерки. В чл. 11, ал. 3 от Закона за нормативните актове изрично е регламентирано, че нормативните актове се отменят,

изменят или допълват с изрична разпоредба на новия, изменящия или допълващия акт.

В тази връзка се предвиждат негативни въздействия, аналогични на посочените във Вариант 0.

6. Положителни въздействия: *Опишете качествено (при възможност – и количествено) всички значителни потенциални икономически, социални, екологични и други ползи за идентифицираните заинтересовани страни за всеки един от вариантите в резултат на предприемане на действията. Посочете как очакваните ползи кореспондират с формулираните цели.*

Вариант 0 "Без действие": При този вариант не са идентифицирани положителни въздействия.

Вариант 1 Приемане на проекта: С приемането на законопроекта ще бъдат предприети мерки за по-добра защита от хакерски атаки и инциденти, насочени към субекти в държавите членки на ЕС, в т.ч. и България, с цел придобиване на чувствителна информация.

Ще се актуализира правната уредба, необходима за предотвратяване на атаки и намесата в мрежови устройства като рутери, комуникатори, защитни стени, мрежово базирани системи за откриване на проникванията (Instrusion Detection Sistem), 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.

Ще бъдат въведени в българското законодателство изцяло изискванията на чл. 9, пар. 4, буква „б" и буква „в" от Директива 2013/40/ЕС относно атаките срещу информационните системи. В разпоредбата на чл. 319г НК ще се предвиди изрична уредба на случаите, когато намесата е насочена срещу информационна система, която е част от критична инфраструктура, което ще бъде в съответствие с изискванията на чл. 9, пар. 4 от Директивата. По този начин ще бъде изпълнено задължението на Република България по процедура за нарушение № 2019/2240 във връзка с официално уведомително писмо на Европейската комисия (ОУП) № С (2019) 6272.

Ще бъде изпълнена мярката, препоръчана от Центъра по киберсигурност към Европол в държавите членки да бъде прилаган закон, който трябва да бъде еднакво дързък, за да отговори на предизвикателството и в тази връзка законодателството на държавите членки да еволюира съобразно постоянно променящите се и развиващи се технологии.

Ще са налице законови основания за по-адекватно противодействие 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. 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 частният сектор да прави вложения в защитени резервни копия на данните, тъй като иначе биха загубили трайно своите данни.

Приемането на законопроекта ще допринесе за повишаването на информационната сигурност чрез въвеждането на по-висока степен на наказателноправна защита срещу извършването на компютърни престъпления, която да съответства на тяхната реална обществена опасност и да способства за ефективното разследване на подобен вид

деяния.

Вариант 2 Предприемане на организационни и други мерки без нормативни промени:

При неприемане на проекта, положителни въздействия върху заинтересованите страни не се очакват.

Определяне на по-значимите въздействия:

Въздействия:	**Вариант 0 - „Без действие“:**	**Вариант 1- „Приемане на предложения проект на акт“:**	**Вариант за действие 2 - „Предприемане на организационни и други мерки без нормативни промени“:**
Повишаване на информационната сигурност чрез въвеждането на по-висока степен на наказателноправна защита срещу извършването на компютърни престъпления	При неприемане на проекта, положителни въздействия върху заинтересованите страни не се очакват. Съвременните информационни технологии и 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.	Ще се актуализира правната уредба необходима за предотвратяване на атаки и намесата в мрежови устройства като рутери, комуникатори, защитни стени, мрежово базирани системи за откриване на проникванията (Instrusion Detection Sistem), 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.	Предприемането на организационни и други мерки без нормативни промени не е достатъчно и нормативно допустимо. Не е възможно предприемането само на организационни и други мерки.

По-добра защита от хакерски атаки и инциденти, които продължават да се насочват към субекти в държавите членки на ЕС, в т.ч. и България, с цел придобиване на чувствителна информация	При неприемане на проекта няма бъде изпълнена мярката, препоръчана от Центъра по киберсигурност към Европол в държавите членки да бъде прилаган закон, който трябва да отговори на съвременните предизвикателства и в тази връзка законодателството на държавите членки да еволюира съобразно постоянно променящите се и развиващи се технологии. Няма да бъдат въведени в българското законодателство изцяло изискванията на чл. 9, пар. 4, буква „б“ и буква „в“ от Директива 2013/40/ЕС относно атаките срещу информационните системи.	Ще бъде изпълнена мярката, препоръчана от Центъра по киберсигурност към Европол в държавите членки да бъде прилаган закон, който трябва да отговори на съвременните предизвикателства и в тази връзка законодателството на държавите членки да еволюира съобразно постоянно променящите се и развиващи се технологии. Ще бъдат въведени в българското законодателство изцяло изискванията на чл. 9, пар. 4, буква „б“ и буква „в“ от Директива 2013/40/ЕС относно атаките срещу информационните системи.	Предприемането на организационни и други мерки без нормативни промени не е достатъчно и нормативно допустимо. Не е възможно предприемането само на организационни и други мерки.

Осигуряване защитата на правата и законните интереси на физическите и юридическите лица	При неприемане на проекта, положителни въздействия върху заинтересованите страни не се очакват. Няма да се допринесе за повишаването на информационната сигурност чрез въвеждането на по-висока степен на наказателноправна защита срещу извършването на компютърни престъпления, която да съответства на тяхната реална обществена опасност и да способства за ефективното разследване на подобен вид деяния.	Приемането на законопроекта ще допринесе за повишаването на информационната сигурност чрез въвеждането на по-висока степен на наказателноправна защита срещу извършването на компютърни престъпления, която да съответства на тяхната реална обществена опасност и да способства за ефективното разследване на подобен вид деяния.	Предприемането на организационни и други мерки без нормативни промени не е достатъчно и нормативно допустимо. Не е възможно предприемането само на организационни и други мерки.
Вероятност въздействието да се прояви – Вариант 1			
Ниска			
Средна			
Висока	X	X	X

7. Потенциални рискове: *Посочете възможните рискове от приемането на нормативната промяна, включително възникване на съдебни спорове:*

Не са налице рискове.

8.1. Административната тежест за физическите и юридическите лица:

☐ Ще се повиши

☐ Ще се намали

X Няма ефект

8.2. Създават ли се нови регулаторни режими? Засягат ли се съществуващи режими и услуги?

Не се създават.

9. Създават ли се нови регистри?

Когато отговорът е „да", посочете колко и кои са те: НЕ се създават.

10. Как въздейства актът върху микро, малките и средните предприятия (МСП)?

☐ Актът засяга пряко МСП

☐ Актът не засяга МСП

X Няма ефект

11. Проектът на нормативен акт изисква ли цялостна оценка на въздействието?

☐ Да

X Не

12. Обществени консултации: *Обобщете най-важните въпроси за консултации в случай на извършване на цялостна оценка на въздействието или за обществените консултации по чл. 26 от Закона за нормативните актове. Посочете индикативен график за тяхното провеждане и видовете консултационни процедури.*

Предвижда се в съответствие с изискванията на чл. 26, ал. 3 и ал. 4 от Закона за нормативните актове, проектът на акт да бъде публикуван на страницата на Министерството на правосъдието в интернет и на Портала за обществени консултации за срок от 30 дни.

13. Приемането на нормативния акт произтича ли от правото на Европейския съюз?

X **Да**

☐ Не

Моля посочете изискванията на правото на Европейския съюз, включително информацията по т. 8.1 и 8.2, дали е извършена оценка на въздействието на ниво Европейски съюз, и я приложете (или посочете връзка към източник):

Приемането на нормативния акт е свързано с осигуряване на пълното транспониране на Директива 2013/40/ЕС относно атаките срещу информационните системи. По проекта на директива от ЕК е била изготвена оценка на въздействието: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010SC1123&from=EN

14. Име, длъжност, дата и подпис на директора на дирекцията, отговорна за изработването на нормативния акт:

Име и длъжност: Любомир Талев, директор на дирекция „Съвет по законодателство"

Дата: 03.06.2020 г.

Подпис: