Образецът на частична предварителна оценка на въздействието влиза в сила от 01 януари 2021 г.

Частична предварителна оценка на въздействието	
Институция: Министерство на електронното управление	**Нормативен акт:** Законопроект за изменение и допълнение на Закона за Киберсигурност
○ Не е включен в законодателна/оперативна програма на Министерския съвет	◉ Включен е в законодателната/оперативната програма на Министерския съвет за: **„Програма за управление на Република България юни 2023 г. – декември 2024 г.** **20.1.10. Одобряване от Министерския съвет и внасяне в Народното събрание на Законопроект за изменение и допълнение на Закона за киберсигурност”**
Лице за контакт: Бисерка Радева	**Телефон и ел. поща:** 02/94942301, b.radeva@egov.government.bg

1. Проблеми за решаване:

Приета е нова Директива (ЕС) 2022/2555 (Директива МИС2), която е част от пакет от мерки за допълнително подобряване на устойчивостта и капацитета за реагиране при инциденти на публичноправните и частноправните субекти, компетентните органи и Съюза като цяло в областта на киберсигурността и защитата на критичната инфраструктура. Тя е съобразена с приоритетите на Комисията за привеждане на Европа в готовност за цифровата ера и за изграждането на приспособена към бъдещите предизвикателства икономика, която работи в интерес на хората. Киберсигурността е приоритет в отговор на Комисията по отношение на кризата с COVID-19. Пакетът включва и нова стратегия относно киберсигурността, имаща за цел укрепване на стратегическата самостоятелност на Съюза за подобряване на неговата устойчивост и колективна реакция, както и за изграждане на отворен и глобален интернет. Наред с гореизброените мерки и директива относно устойчивостта на критичните оператори на основни услуги, имаща за цел да ограничи физическите заплахи срещу такива оператори.

Директива МИС2 надгражда и отменя Директива (ЕС) 2016/1148 за сигурност на мрежите и информационните системи (Директивата за МИС, транспонирана в сега действащия Закон за киберсигурност), която е първата част от общото за целия ЕС законодателство за киберсигурността и която предоставя правни мерки за повишаване на цялостното ниво на киберсигурността в Съюза. Директивата за МИС:

1) допринесе за подобряване на способностите в областта на киберсигурността на национално равнище посредством изискването от държавите членки да приемат национални стратегии за киберсигурност и да определят органи в тази сфера;

2) засили сътрудничеството между държавите членки на равнището на Съюза, като въведе различни форуми, улесняващи обмена на стратегическа и оперативна информация; и

3) подобри киберустойчивостта на публичноправните и частноправните субекти в седем конкретни сектора (енергетика, транспорт, банково дело, инфраструктури на финансовия пазар, здравеопазване, доставка и снабдяване с питейна вода и цифрови инфраструктури), както и в рамките на три цифрови услуги (онлайн местата за търговия, онлайн търсачките и компютърните услуги „в облак“), изисквайки от държавите членки да гарантират, че операторите на основни услуги и доставчиците на цифрови услуги са въвели изисквания за киберсигурност и докладват за инциденти.

С Директива МИС2 се осъвременява съществуващата правна рамка, като се отчитат повишената цифровизация на вътрешния пазар през последните години и развиващата се картина на заплахите за киберсигурността. Тези две тенденции на развитие се засилиха допълнително след началото на кризата с COVID-19. Директива МИС2 предвижда и действия по отношение на някои слабости, които попречиха на Директивата за МИС да разгърне пълния си потенциал.

Независимо от постиженията на Директивата за МИС, която проправи пътя за значителна промяна в нагласите във връзка с институционалния и регулаторния подход към киберсигурността в редица държави членки, проличаха и нейните ограничения. Цифровата трансформация на обществото (ускорена от кризата с COVID-19) разшири картината на заплахите и породи нови предизвикателства, изискващи новаторски решения за реакция. Кибератаките идват от широк кръг източници в ЕС и извън него, а броят и сложността им продължава да нараства.

В оценката за функционирането на Директивата за МИС, извършена за целите на оценката на въздействието, бяха установени следните проблеми:

1) ниското ниво на киберустойчивост на предприятията, извършващи дейност в ЕС;

2) нееднаквите нива на устойчивост в отделните държави членки и сектори; както и

3) ниското ниво на съвместна ситуационна осведоменост и липса на съвместна реакция при кризи. Например, някои главни болници в някои държави членки не попадат в обхвата на Директивата за МИС, поради което от тях не се изисква да прилагат произтичащите мерки за сигурност, докато в други държави членки почти всеки доставчик на здравно обслужване е обхванат от изискванията за сигурност на МИС.

Като инициатива в рамките на Програмата за пригодност и резултатност на регулаторната рамка (REFIT) предложението има за цел да намали регулаторната тежест за компетентните органи и разходите на публичноправните и частноправните субекти за привеждане в съответствие. Това най-вече се постига чрез премахване на задължението на компетентните органи да установяват операторите на основни услуги и чрез увеличаване на нивото на хармонизация на изискванията за сигурност и докладване, с цел да се улесни спазването на регулаторните изисквания за субектите, предоставящи трансгранични услуги. Същевременно, на компетентните органи ще бъдат възложени редица нови задачи, включващи надзор върху субектите, които до момента не са обхванати от Директивата за МИС.

<u>По Проблем 1</u>

Необходимост от транспониране на Директива(ЕС) 2022/2555 (Директива МИС2) поради непълно съответствие на действащата нормативна уредба, липса на съгласуваност с действащите разпоредби в тази област на политиката.

Директивата за МИС 2 е част от по-широк набор от съществуващи правни инструменти и предстоящи инициативи на равнището на Съюза, имащи за цел да повишат устойчивостта на публичноправните и частноправните субекти срещу заплахи.

В областта на киберсигурността това са най-вече Директива (ЕС) 2018/1972 за установяване на Европейски кодекс за електронни съобщения (чиито свързани с киберсигурността разпоредби ще бъдат заменени с разпоредбите на разглежданото предложение) и предложението за Регламент относно оперативната устойчивост на цифровите технологии във финансовия сектор Регламент

(ЕС) 2022/2554 и Директива (ЕС) 2022/2556, което се счита за lex specialis за разглежданото предложение.

В областта на физическата сигурност предложението допълва предложението за Директива относно устойчивостта на критичните субекти, с която се преработва Директива 2008/114/ЕО относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита (Директивата за ЕКИ), създаваща в Съюза процес на установяване и означаване на европейски критични инфраструктури и определяща подход за подобряване на тяхната защита. През юли 2020 г. Комисията прие стратегията на ЕС за киберсигурност, в която се признава нарастващата взаимосвързаност и взаимозависимост между физическите и цифровите инфраструктури. В нея се подчертава нуждата от по-съгласуван и последователен подход между Директивата за ЕКИ и Директива МИС.

Ето защо Директива за МИС 2 е тясно съгласувана с предложението за Директива относно устойчивостта на критичните субекти, имаща за цел да повиши устойчивостта на този вид субекти срещу физическите заплахи в голям брой сектори. Предложението цели да гарантира, че компетентните органи съгласно двата правни акта при необходимост предприемат допълнителни мерки и обменят информация относно устойчивостта в киберпространството и извън него, както и че особено критичните оператори в секторите, които следва да се считат за „основни“ съгласно разглежданото предложение, са предмет и на по-общи задължения за подобряване на устойчивостта с акцент върху рисковете извън киберпространството. Това налага да бъде актуализирано и българското законодателство в областта, чрез транспониране на Директивата МИС 2 в Закона за киберсигурност.

Съгласуваност с други политики на Съюза

За Европа и в частност за България е от решаващо значение да се възползва от всички предимства на цифровата ера и да укрепи своята промишленост и иновационен капацитет в рамките на безопасни и етични граници. В Европейската стратегия за данните се определят четири стълба — защита на данните, основни права, безопасност и киберсигурност — като основни необходими условия за общество, което разполага с възможността за използване на данни.

Комисията осигури съгласувани правила за пазарните оператори и улесни създаването на сигурен, надежден и подходящ обмен на информация относно заплахите и инцидентите, за да се търсят възможности за по-добра устойчивост на киберпространството и по-ефективни мерки за противодействие на кибератаките, особено по отношение на основните икономически и обществени дейности, като същевременно се зачитат правомощията на държавите членки, включително отговорността за тяхната национална сигурност . Освен това Директивата МИС 2 не засяга прилагането на правилата за конкуренция, предвидени в Договора за функционирането на Европейския съюз (ДФЕС).

<u>По Проблем 2</u>

Необходимостта от изграждане на координиран подход относно Директива (ЕС) 2022/2555, насочена към изграждане на способности за киберсигурност в целия Съюз, смекчаване на заплахите за сигурността на мрежите и информационните системи, използвани за предоставяне на основни услуги в ключови сектори, и осигуряване на приемственост на такива услуги при изправяне пред тях инциденти с киберсигурност, като по този начин допринася за ефективната икономика и общество на Съюза.

Съгласно българското законодателство, по-специално Закона за киберсигурност, се постигна значителен напредък в областта на национално ниво, а и се повиши нивото на устойчивост на киберсигурността на Съюза. Българският закон послужи за катализатор на институционалния и регулаторен подход към киберсигурността, като изгради основите за значителна промяна в

съществуващите до момента практики и процеси. Директивата МИС, която послужи за основа на Закона за киберсигурност, даде основен тласък за поправката и обновяването и на националната стратегия за киберсигурност, установяване и преразглеждане на национални способности, органи и институции, а и прилагане на нови регулаторни мерки, обхващащи основни инфраструктури и субекти, дефинирани по определен ред и ефективно със съвременните и възникващи предизвикателства в областта на киберсигурността.

Мрежовите и информационните системи се превърнаха в централна характеристика на ежедневието с бързата цифрова трансформация и взаимосвързаността на обществото, включително при трансграничния обмен. Това развитие доведе до разширяване на екосистемата на киберсигурността, като предизвика нови предизвикателства, които изискват адаптирани, координирани и иновативни отговори във всички държави-членки. Броят, големината, усъвършенстваността, честотата и въздействието на инцидентите в киберсигурността се увеличават и представляват основна заплаха за функционирането на мрежовите и информационните системи. В резултат на това кибер инцидентите могат да възпрепятстват осъществяването на икономически дейности на вътрешния пазар и да генерират финансови загуби. Следователно готовността и ефективността на киберсигурността са по-важни от всякога за правилното функциониране на вътрешния пазар.

С транспонирането на директивата се адресират гореизложените проблеми, като се подобряват възможностите за:

1. Премахване на фрагментацията на вътрешния пазар, която влияе негативно на функционирането, трансграничните услуги и нивото на устойчивост на киберсигурността поради прилагането на различни стандарти. С приемането на единен критерий, а именно правилото за ограничаване на размера, всички средни и големи предприятия, както са определени в Препоръка 2003/361/ЕО на Комисията, които работят в секторите или предоставят вида на услугите, обхванати от директивата, попадат в обхвата. Това на практика определя всички субекти в регулацията по киберсигурност.

От една страна ДЧ не са задължени да съставят списък на субектите, които отговарят на този общоприложим критерий, свързан с размера – средните и големите предприятия, докато що касае малките или микросубектите, с ключова роля за икономиките или обществата, попадащи в обхвата на директивата, при транспониране ДЧ трябва да съставят списък за тях. Това до голяма степен ще наложи допълнителни ограничения за субектите, както и административна тежест за икономиката и бизнеса.

2. Класификацията на секторите в две категории: „съществени“ и „важни“. Тази категоризация отчита нивото на критичност на сектора или вида на услугата, както и нивото на зависимост на други сектори или видове услуги. Досега, опитът ни показва колко е трудно да се направи такова разделение на национално ниво. Имаме изградена система за разпределение на секторите на критични и на стратегически обекти.Преминаването към нова класификация ще отнеме определен административен ресурс, както и определено време. Доброволното сътрудничество между отговорните институции, мерките за общо прилагане и взаимодействие е подходящо да бъдат подсилени, но от гледна точка на правоприлагането на национално ниво ще се изисква допълнително време за усъвършенстване на процеса.

3. ДЧ обмислят функционално разделение между оперативните задачи, предоставени от ЕРИКС (обмена на информация и подкрепата за субекти) и надзорните дейности на компетентните органи. Това в някаква степен означава да бъде създаден нов национален надзорен, административен наказателено-процесуален орган, или компетенциите да бъдат възложени на съществуващ такъв.

4. Създаването на Координационен ЕРИКС, обмена на служители, обединяването на взаимодействието между EU-CyCLONe и мрежата CSIRTs, определянето на повече от един НКО,

отговорен за изпълнението на задачите, свързани със сигурността на МИС на съществени и важни субекти съгласно директивата, широкото сътрудничество с академични и изследователски институции, въвеждането на механизъм за партньорска проверка, позволяващ оценка от експерти, определени от държавите-членки, на прилагането на политиките за киберсигурност, включително нивото на способностите на държавите-членки и наличните ресурси и др. са все мерки които изискват наличие на заявен политически модел на взаимодействие, на една развита и работеща в пълен обем национална кибер система, каквато малките ДЧ все още нямат.

5. Скоростното развитие на цифровия свят и дигиталната глобализация доведе до злоупотреби, превръщащи се в масови престъпления, допълнени от кризата с COVID-19 се създадоха индикации за обостряне на световните проблеми в кибер пространството.

Няколко основополагащи разлики в досега съществуващият кибер регулационен режим: създаването на правила за сътрудничество между компетентните органи и надзорните органи в съответствие с Регламент (ЕС) 2016/679 за справяне с нарушения, свързани с лични данни, както и осигуряването на високо ниво на отговорност за мерките за управление на риска в киберсигурността и задълженията за докладване на ниво организации.

По Проблем 3

Допълване на основни сегменти, както и разширяване на икономическите сектори съгласно Директива (ЕС) 2022/2555, осъществяване на регулацията им посредством надграждане дейността и добавяне на правомощия на националните компетентни органи

Управителните органи на субектите, попадащи в обхвата, следва да одобрят мерките от риска за киберсигурност и да контролират тяхното прилагане, също и управлението на риска, сертификацията по специфични европейски схеми за сертифициране на киберсигурността, като обособяването и прецизирането на Административнонаказателените разпоредби, респективно органите, които да гарантират:

- ефективно наблюдение;

- да следи за изпълнението и предприемането на необходимите мерки, за спазването на правилата, които са ефективни, пропорционални и възпиращи, като се вземат предвид обстоятелствата за всеки отделен случай чрез:

  - проверки на място и надзор извън обекта, включително произволни проверки;

  - редовни одити; целенасочени одити на сигурността въз основа на оценки на риска или свързана с риска налична информация;

  - сканиране за сигурност, основаващо се на обективни, недискриминационни, справедливи и прозрачни критерии за оценка на риска;

  - искания за информация, необходима за оценка на мерките за киберсигурност, приети от субектите, включително документирани политики за киберсигурност, както и спазването на задължението за уведомяване на ENISA съгласно член 25, параграфи 1 и 2;

  - искания за достъп до данни, документи или каквато и да е информация, необходима за изпълнението на техните надзорни задачи; искания за доказателства за прилагане на политики за киберсигурност, като например резултатите от одитите за сигурност, извършени от квалифициран одитор, и съответните основни доказателства.

Създаването на надзорни органи ще създаде тежест и за бизнеса, и за администрацията. Санкционните режими, възможността за суспендиране на правомощия изграждат един изцяло нов и утежнен административен процес. Вменяването на нови и широки правомощия у административнонаказващите органи ще доведе до забавяне процесите по изпълнение на мерките за киберзащита и ще увеличи рисковете за бизнеса и икономиката. Гарантирането на

ефективността им ще бъде дълъг и трудоемък процес. Предприемането на необходимите действия за отстраняване на недостатъците в определения срок, преустановяване сертифицирането или разрешението налагат или изискват налагането от съответните органи или съдилища съгласно националното законодателство на временни забрани срещу субектите, а определянето на действителните причинени вреди или претърпени загуби или потенциални щети или загуби, които биха могли да бъдат предизвикани, изисква сериозна експертиза и административен опит в киберсигурността или МИС.

Всичко това определя важността на транспонирането на Директивата на национално ниво и необходимостта на новосъздадените правила да залегнат дългосрочно в законодателството в областта на киберсигурността на страната.

В основата си транспонирането на Директивата заляга върху възможността за продължаване на някои съществуващи практики, за надграждане на други основни сегменти, както и допълване и разширяване на икономически сектори. Не трябва да се забравя, че секторите и към настоящия момент в закона не са малко, допълването има на практика с два нови подсектора и десет изцяло нови сектора, ще разшири обхвата, но на практика няма да промени основно и сега съществуващите браншове и сектори в страната.

3.1. Описание на проблемите, които се уреждат с проекта на ЗИД на ЗКС. Описание на причините за тяхното възникване

До приемането на Директива (ЕС) 2021/2555 европейската правна рамка, обхващаща киберсигурността, свързана с ИКТ е фрагментирана и непълна. В някои сектори (транспорт, здравеопазване, енергетика и т.н.) са предвидени специфични и подробни разпоредби за постигане на минимална сигурност на мрежите и информационните системи. Други сектори, обаче, не попадаха в обхвата на първия законов акт. Въпреки, че България постъпи иновативно включвайки сектор администрация още в първия закон за киберсигурност, при Директива МИС 2, той се явява задължителен. Определянето на субектите се случва посредством нарочна методология, докато в новата регулация ще бъде дефинирано по техния размер, спрямо Закона за малките и средни предприятия.

Вменяването на задължения на нови органи и функции ще създаде известна тежест за бизнеса и администрацията, както и новите санкционни режими, но проектът на нормативен акт ще съдейства за пренасяне на положителен ефект в киберпрактиката на национално ниво.

3.2. Описание на проблемите в прилагането на съществуващото законодателство

Към момента в България е налице нормативна регламентация на киберсигурността, съществуват национални компетентни органи и национални НЕРИКС и СЕРИКС-и в адаптираните сектори в обхвата на старата Директива 1148/2016. Разширяването на обхвата по Директива МИС2 ще доведе неминуемо до създаване на нови компетентни органи в новоприетите сектори. Както и в останалите държави членки, това би могло да се постигане посредством гарантирането, че отговорните секторни институции разполагат с достатъчно финансов ресурс за покриване на новосъздадените рискове и задължения. По подобие на останалите държави членки в ЕС, и в България са налице празноти или припокривания във важни области (например при докладването на инциденти) наблюдава се икономически неефективно прилагане на припокриващи се правила.

С новия проект на закон ще се избегнат неяснотите относно задълженията за докладване, ще се осигури ясна и дефинирана линия за разпределяне на отговорността при компетентните органи по сектори. По този начин ще се посрещнат предизвикателствата на разширения кръг от субекти и новите надзорни регулации.

3.3. Описание на нововъзникналите обстоятелства

За да се преодолее недостатъчната законова уредба от гледна точка на разгръщане на секторите, създаване на нови регулаторни функции, както и правила за управление на риска, свързан с ИКТ, в т.ч. за да се осигурят мерки по прилагането на Директива (ЕС) 2022/2555 и да се въведат предвидените изменения в националното законодателство, е необходимо в срок до 17 октомври 2024 г., да се измени съществуващият Закон за киберсигурност. Въз основа на спецификите в полето на киберсигурността, регулирани с европейския акт, видовете субекти, попадащи в обхвата, случаите на въведен по-лек режим на оценка на риска и докладване за някои от тях и на изключените от приложното им поле субекти, и не на последно място при отчитане на действащото българско законодателство, ще се наложат изменения в Закона за киберсигурност, Закона за електронните съобщения.

В Директива (ЕС) 2022/2555 на държавите членки са предоставени няколко опции, които следва да бъдат обстойно преценени преди Република България да реши да се възползва или да не се възползва от една от тях, а именно:

- в чл. 2, параграф 5, Директива (ЕС) 2022/2555 на държавите членки е посочено, че могат да предвидят настоящата директива да се прилага за:

а) органи на публичната администрация на местно равнище;

б) образователни институции, по-специално когато извършват научноизследователски дейности от критично значение.

- В чл. 8, параграф 1, от Директива (ЕС) 2022/2555 е посочено, че държавите членки могат: „… определя или създава един или повече компетентни органи, отговарящи за киберсигурността и за надзорните задачи, посочени в глава VII" („компетентни органи").

В тази връзка, измененията в действащия закон са свързани с надграждане ролята на националните компетентни органи и създаване и допълване на секторни компетентни органи, съответстващи на новите приобщени сектори в Приложението.

2. Цели:

Цел 1: Повишаване степента на подготвеност на съществените и важни субекти в областта на киберсигурността

Това би довело до смекчаване на потенциалните загуби на приходи поради кибератаки и би намалило големите разходи за смекчаване на заплахите ad-hoc. Подобни ползи вероятно ще надделеят над необходимите инвестиционни разходи. Намаляването на фрагментирането на вътрешния пазар би подобрило и условията на равнопоставеност сред операторите.

За държавите членки то допълнително би намалило риска от увеличаване на бюджетните разходи за смекчаване на заплахите ad-hoc и допълнителните разходи в случай на извънредни ситуации, свързани с инциденти с киберсигурността.

Общата цел е да се обезпечи правната интеграция на българската киберсигурност с европейската, в т.ч. посредством въвеждането на подобрените европейски изисквания във връзка с оценката на риска например.

Конкретната цел е да се запълнят констатираните празноти и отстранят несъответствията в действащото българско законодателство чрез въвеждането на правила за капацитета за оценка на риска, докладването на инциденти, тестването, повишаването на осведомеността и осъзнатостта на факта, че киберинцидентите и липсата на адекватен отговор могат да застрашат стабилността както на публичните, така и на частните субекти.

Оперативната цел на предложените промени в националното законодателство е в него да се въведат мерки за прилагането на Директива (ЕС) 2022/2555.

Цел 2: Допълване и усъвършенстване на съществуващия нормативен режим за съществените и важни субекти в съответствие с изискванията на Директива (ЕС)2022/2555

С оглед ангажиментите, произтичащи от членството на Република България в ЕС, във връзка с транспонирането на изискванията на Директива (ЕС) 2022/2555 в националното законодателство, необходимо е да бъдат предприети мерки за прецизиране на нормативната уредба и създаване на ясен и ефективен режим, който да регулира задълженията на съществените и важни субекти в съответствие с въведените в директивата по-високи изисквания при постигане на киберсигурността на субектите, при запазване на изискванията за защита на мрежите и информационните системи. В Директивата са предвидени общи цели за дейността по отношение на ново-обхванатите сектори, главно поради:

• повишената цифровизация през последните години и по-високата степен на взаимосвързаност,

• факта, че понастоящем този обхват вече не отразява всички цифровизирани сектори, предоставящи ключови услуги за икономиката и обществото като цяло.

- обхвата на операторите на основни услуги, да бъде изяснен в достатъчна степен с оглед на доставчиците на цифрови услуги, идентифицирани като такива във всички държави членки, с цел да въвеждат мерки за сигурност и да докладват за инциденти;
- уеднаквяване на определянето на изискванията за сигурност и докладването на инциденти;
- режимът на надзор и правоприлагане, налагане на санкции на субекти, които не са въвели изискванията за сигурност или не са докладвали за инциденти;
- покачване равнището на зрялост при справяне с рисковете за киберсигурността;
- систематичният обмен на информация с цел подобряване на ефективността на мерките за киберсигурност и за степента на съвместна ситуационна осведоменост на равнището на ЕС. Случаят е такъв и при обмена на информация между частноправни субекти, както и при обмена между структурите за сътрудничество на равнището на ЕС и частноправните субекти.

Конкретната цел е да се запълнят констатираните празноти и отстранят несъответствията в действащото българско законодателство чрез изясняване обхвата на съществени и важни субекти, оператори на основни услуги, прецизиране на надзорния режим, надграждане систематичния обмен на информация между заинтересованите субекти както на публичните, така и на частните субекти.

Оперативната цел на предложените промени в националното законодателство е в него да се въведат мерки за прилагането на Директива (ЕС) 2022/2555.

Цел 3 Адаптиране на съществуващата нормативна рамка в ЗКС в съответствие с изискванията на Директива (ЕС) 2022/2555, както и разширяване на компетенциите на компетентните органи по киберсигурност в Р България

В действащото национално законодателство трябва да бъде предвиден правен режим за осъществяване регулацията на новите сектори в обхвата на Директива МИС 2, което да подсигури еднакво третиране на субектите ѝ и правна сигурност.

Една от основните цели на Директива (ЕС) 2022/2555 е именно осигуряването на високи гаранции и възможности за по-добра устойчивост на киберпространството и по-ефективни мерки за противодействие на кибератаките, особено по отношение на основните икономически субекти и държавните органи. В този смисъл новите регулации целят гарантиране на справедливо третиране на субектите, повишаване на тяхната информираност и осигуряване на надежден и ефективен надзор за спазване на правата и законните им интереси. Това може да се осъществи чрез възлагане на допълнителни правомощия в полза на компетентните в областта органи и усъвършенстването на съществуващата нормативна уредба което ще подсигури постигането на следните конкретни цели:

- предвиждане на допълнителни мерки, свързани със справедливото третиране на кредитополучателите, повишаване на тяхната информираност и осигуряване на надежден и ефективен надзор за спазване на правата и законните им интереси;
- Доклад на цялостна предварителна оценка на въздействието
- регламентиране на процедури за сътрудничество и обмен на информация между компетентните органи и НЕРИКС, ЕРИКС;
- предвиждане на задължение за докладване на инциденти;
- въвеждане на задължение за наличие на подходящи политики и процедури повишаване киберсигурността и способността на дружествата и органите да отговорят бързо на инцидент и да ограничат въздействието му.

Цел 4: Регулация на присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на Административнонаказателен орган (Национален компетентен орган)

В националното законодателство е нужно да се въведе цялостна уредба относно изискванията за киберсигурност и условия за управление и противодействие на рисковете касаещи съществените и важни субекти, както и отговарящите на зададените критерии, попадащи в определените сектори в Приложение 1 и 2. На компетентните органи се предоставят широки пълномощия по управление и надзор политиките по киберсигурност по отношение на определените субекти – съществени и важни. Компетентните органи следва да бъдат оправомощени да прилагат санкции, състоящи се в спиране на сертифициране или разрешение относно част или всички услуги пропорционално на тежестта на нарушението, само като ultima ratio, което означава само след изчерпване на другите съответни действия по прилагане, за времето, докато субектите, спрямо които се прилагат, предприемат необходимите действия за отстраняване на недостатъците. След установен минимален списък на административните санкции за нарушаване на задълженията за управление на риска от киберсигурност и докладване, се създава ясна и последователна рамка за санкциите, според естеството, тежестта и продължителността на нарушението, действителните причинени вреди или нанесените загуби или потенциални щети или загуби, които биха могли да бъдат предизвикани, умишлен или небрежен характер на нарушението, действията, предприети за предотвратяване или смекчаване на претърпени вреди и/или загуби, степента на отговорност или съответните предишни нарушения, степента на сътрудничество с компетентния орган и всеки друг утежняващ или смекчаващ фактор. Всеки компетентен орган следва да има правомощието да налага административни глоби и в тази връзка следва да се създаде система, която предвижда ефективни, пропорционални и възпиращи санкции. Естеството на такива наказания, наказателни или административни, се определя в ЗИД на ЗКС. Като допълнение ще се насърчи обменът на данни за заплахите, спазването на мерките за управление на риска в областта на киберсигурността и задълженията за докладване и т.н.

•Пригодност и опростяване на законодателството

Директива (ЕС) 2022/2555 предвижда общо изключване на микросубектите и малките субекти от обхвата на МИС и по-лек надзорен режим с последващ (ex-post) надзор, прилаган спрямо голям брой от новите субекти съгласно преразгледания обхват (т. нар. важни субекти). Цел на мерките е да сведат до минимум и да балансират тежестта, на която са подложени дружествата и органите на публичната администрация, както и замяната на сложната система за установяване на операторите на основни услуги с общоприложимо задължение и въвеждане на по-високо ниво на хармонизация на задълженията за сигурност и докладване, което би намалило тежестта за изпълнение, особено за субекти, предоставящи трансгранични услуги.

Целта на новата е регулация е да се сведат до минимум разходите за привеждане в съответствие на малките и средните предприятия, тъй като от субектите се изисква да предприемат само онези мерки, необходими за гарантиране на ниво на сигурност на мрежите и информационните системи, които съответстват на съществуващия риск.

•Основни права

ЕС има ангажимент да осигури високи стандарти за защита на основните права. Всички насърчавани доброволни договорености за обмен на информация между субектите биха се осъществявали в надеждна среда при пълно спазване на разпоредбите на Съюза за защита на данните, и особено на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета.

•Планове за изпълнение и механизъм за мониторинг, оценка и докладване

В общия план за мониторинг и оценка на въздействието върху конкретните цели е включено докладване от Европейската Комисия на Европейския парламент и на Съвета на своите основни констатации, което изисква да бъде извършен преглед поне [54 месеца] след датата на влизане в сила на акта.

Прегледът трябва да се извърши в съответствие с Насоките на Комисията за по-добро законотворчество.

•Подробно разяснение на конкретните разпоредби на предложението

Предложението е структурирано около няколко основни области на политиките, които са взаимосвързани и служат на целта да се повиши нивото на киберсигурност в Съюза.

Предмет и обхват (членове 1 и 2)

Директивата, по-специално:

а) установява задължения за държавите членки да приемат национална стратегия за киберсигурност, да определят компетентни национални органи, единни звена за контакт и ЕРИКС;

б) предвижда държавите членки да определят за субектите, обозначени като съществени в Приложение I и като важни в Приложение II, задължения за управление на свързания с киберсигурността, и за докладване;

в) предвижда държавите членки да определят задължения относно обмена на информация за киберсигурността.

Директивата се прилага по отношение на някои публичноправни или частноправни съществени субекти, упражняващи дейност в изброените в Приложение I сектори (енергетика; транспорт; банково дело; инфраструктури на финансовия пазар; здравеопазване, питейна вода; отпадъчни води; цифрова инфраструктура; публична администрация и космическо пространство), както и на някои важни субекти, упражняващи дейност в изброените в Приложение II сектори (пощенски и куриерски услуги; управление на отпадъците; производство на изделия и вещества и дистрибуция на химикали; производство, преработка и разпространение на храни; производствени и цифрови доставчици). Микропредприятията и малките предприятия по смисъла на Препоръка 2003/361/ЕО на Комисията от 6 май 2003 г. са изключени от обхвата на Директивата, с изключение на доставчиците на електронни съобщителни мрежи или на общественодостъпни електронни съобщителни услуги, доставчиците на удостоверителни услуги, регистрите на имената на домейни от първо ниво (TLD) и публичната администрация, както и на някои други субекти, като например единствени доставчици на дадена услуга в дадена държава членка.

Национални рамки за киберсигурност (членове 5—11)

От държавите членки се изисква да приемат национална стратегия за киберсигурност, в която са определени стратегическите цели и подходящи мерки на политиката, както и подходящи регулаторни мерки за постигане и поддържане на високо ниво на киберсигурност.

Директивата установява и рамка за координирано оповестяване на уязвимости и изисква държавите членки да определят ЕРИКС, които да действат като надеждни посредници и да улесняват взаимодействието между докладващите субекти и производителите или доставчиците на ИКТ продукти и услуги. ENISA трябва да разработи и поддържа Европейски регистър на уязвимостите за откритите такива.

От държавите членки се изисква да въведат национални рамки за управление на кризи в областта на киберсигурността, по-специално чрез определяне на национални компетентни органи, отговарящи за управлението на мащабни инциденти и кризи в тази област.

От държавите членки се изисква и да определят един или повече национални компетентни органи по киберсигурност за надзорните задачи съгласно настоящата директива, както и национално единно звено за контакт по киберсигурността (НЕЗК), което да изпълнява функция на свръзка, за да се осигури трансгранично сътрудничество на органите на държавите членки. От държавите членки се изисква също така да определят екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС).

Сътрудничество (членове 12—16)

С Директивата се създава Група за сътрудничество с цел подкрепа и улесняване на стратегическото сътрудничество и обмен на информация между държавите членки и изграждане на доверие сред тях. Създава се и мрежа на ЕРИКС, с цел да се допринесе за изграждането на доверие между държавите членки и да се насърчи бързото и ефективно оперативно сътрудничество.

Създава се Европейска мрежа за връзка на организациите при кибер кризи (EU — CyCLONe) с цел подпомагане на координираното управление на мащабни инциденти и кризи, свързани с киберсигурността, и осигуряване на редовния обмен на информация сред държавите членки и институциите на ЕС.

От ENISA се изисква да публикува в сътрудничество с Комисията двугодишен доклад за състоянието на киберсигурността в Съюза.

От Комисията се изисква да установи система за партньорска проверка, позволяваща редовни такива проверки на ефективността на политиките на държавите членки в областта на киберсигурността.

Управление на риска, свързан с киберсигурността, и задължения за докладване (членове 17—23)

Директивата изисква от държавите членки да гарантират, че управителните органи на всички субекти в обхвата одобряват мерките за управление на риска за киберсигурността, предприети от съответните субекти, и преминават свързано с киберсигурността специфично обучение.

От държавите членки се изисква да гарантират, че попадащите в обхвата субекти предприемат подходящи и пропорционални технически и организационни мерки за управление на рисковете за киберсигурността на мрежите и информационните системи. Те трябва да гарантират също, че субектите уведомяват националните компетентни органи или ЕРИКС за всеки инцидент с киберсигурността, оказващ значимо въздействие върху предоставяната от тях услуга.

В регистрите на имената на домейни от първо ниво (TLD) и субектите, предоставящи услуги за регистриране на имена на домейни от първо ниво, следва да се събират и поддържат точни и пълни данни за регистрацията на имена на домейни. Освен това от тези субекти се изисква да предоставят ефикасен достъп до данните за регистрация на домейни за законно търсещите достъп.

Юрисдикция и регистрация (членове 24 и 25)

По правило съществените и важните субекти се считат за попадащи под юрисдикцията на държавата членка, в която предоставят услугите си. Някои видове субекти обаче (доставчиците на DNS услуги, регистрите на имена на домейни от първо ниво, доставчиците на компютърни услуги „в облак“, доставчиците на услуги на центрове за данни и доставчиците на мрежи за предоставяне на съдържание, както и някои доставчици на цифрово съдържание) се считат за попадащи под юрисдикцията на държавата членка, в която се намира основното им място на установяване в Съюза. Целта е да се гарантира, че тези субекти не се сблъскват с множество различни правни изисквания, тъй като те в особено висока степен предлагат трансгранични услуги. ENISA трябва да създаде и поддържа регистър на последния вид субекти.

Обмен на информация (членове 26 и 27)

Държавите членки трябва да предвидят разпоредби, позволяващи на субектите да участват в свързан с киберсигурността обмен на информация в рамките на конкретни договорености за обмен на информация за киберсигурността, в изпълнение на член 101 от ДФЕС. Освен това

държавите членки трябва да позволят на субектите извън обхвата на настоящата директива да докладват доброволно значими инциденти, киберзаплахи или ситуации, близки до инциденти.

Надзор и правоприлагане (членове 28 и34)

От компетентните органи се изисква да упражняват надзор върху субектите, попадащи в обхвата на директивата, и по-специално да гарантират спазването от тяхна страна на изискванията за сигурност и уведомяване за инциденти. Разграничава се между режим на предхождащ надзор (ex-ante) за съществените субекти и режим на последващ надзор (ex-post) за важните субекти, като във втория случай от компетентните органи се изисква да предприемат действия, когато са получили доказателства или индикации, че значим субект не спазва изискванията за сигурност и уведомяване за инциденти.

Директивата изисква от държавите членки също да налагат административни глоби на съществените и важните субекти и да определят някои максимални глоби.

От държавите членки се изисква при необходимост да си сътрудничат и да се подпомагат взаимно, когато субектите предоставят услуги в повече от една държава членка или когато основното място на установяване на субекта или негов представител се намира в дадена държава членка, но неговите мрежи и информационни системи са разположени в една или повече други държави членки.

2020/0359 (COD)

Посочете определените цели за решаване на проблема/проблемите, по възможно най-конкретен и измерим начин, включително индикативен график за тяхното постигане. Целите е необходимо да са насочени към решаването на проблема/проблемите и да съответстват на действащите стратегически документи.

3. Заинтересовани страни:

1.1. Засегнати субекти:

1. Производители съгласно определението в член 2, точка 38 от Директива (ЕС) 2019/944;
2. Номинирани оператори на пазара на електроенергия съгласно определението в член 2, точка 8 от Регламент (ЕС) 2019/943;
3. Участници на пазара съгласно определението в член 2, точка 25 от Регламент (ЕС) 2019/943, предоставящи услуги за агрегиране, оптимизация на потреблението или съхраняване на енергия съгласно определението в член 2, точки 18, 20 и 59 от Директива (ЕС) 2019/944;
4. Оператори на зарядна точка, отговарящи за управлението и експлоатацията на зарядна точка, която предоставя услуга за зареждане с електроенергия на крайни ползватели, включително от името и за сметка на доставчик на услуги за мобилност;
5. Оператори на районни отоплителни системи или районни охладителни системи съгласно определението в член 2, точка 19 от Директива (ЕС) 2018/2001;
6. Централни структури за управление на запасите съгласно определението в член 2, буква е) от Директива 2009/119/;
7. Оператори в областта на производството, съхранението и преноса на водород;
8. Референтни лаборатории на ЕС съгласно определението в член 15 от Регламент (ЕС) 2022/2371;
9. Субекти, извършващи научноизследователска и развойна дейност в областта на лекарствените продукти, съгласно определението в член 1, точка 2 от Директива 2001/83/ЕО;

10. Субекти, произвеждащи основни фармацевтични продукти и препарати, съгласно определението в раздел B, разделение 21 на NACE Rev. 2;
11. Субекти, произвеждащи медицински изделия, които се считат за критично важни при извънредни ситуации в областта на общественото здраве („списък на критично важните медицински изделия при извънредни ситуации в областта на общественото здраве“), съгласно определението в член 22 от Регламент (ЕС) 2022/123;
12. Предприятия, които събират, обезвреждат или пречистват градски, битови или промишлени отпадъчни води съгласно определението в член 2, точки от 1, 2 и 3 от Директива 91/271/ЕИО, с изключение на предприятията, за които събирането, обезвреждането или пречистването на градски, битови или промишлени отпадъчни води е несъществена част от тяхната обща дейност;
13. - Доставчици на точки за обмен в интернет;
    - Доставчици на DNS услуги, с изключение на оператори на коренови сървъри за имена;
    - Регистри на имената на домейни от първо ниво;
    - Доставчици на услуги за изчисления в облак;
    - Доставчици на услуги на центрове за данни;
    - Доставчици на мрежи за доставка на съдържание;
    - Доставчици на удостоверителни услуги;
    - Доставчици на обществени електронни съобщителни мрежи;
    - Доставчици на обществено достъпни електронни съобщителни услуги;
    - Доставчици на управлявани услуги;
    - Доставчици на управлявани услуги за сигурност;
14. Оператори на наземна инфраструктура, притежавани, управлявани и експлоатирани от държавите членки или от частни лица, които подпомагат предоставянето на космически услуги, с изключение на доставчиците на обществени електронни съобщителни мрежи;
15. Пощенски и куриерски услуги;
16. Управление на отпадъците;
17. Производство, изготвяне и дистрибуция на химикали - Предприятия, извършващи производство на вещества и дистрибуция на вещества или смеси;
18. Производство, преработка и разпространение на храни „предприятие за производство на храни“ означава всяко предприятие с или без стопанска цел, обществено или частно, което извършва някоя от дейностите, свързани с който и да било етап на производство, преработка и разпространение на храни;
19. Производство:

а) Производство на медицински изделия и медицински изделия за инвитро диагностика- Субекти, произвеждащи медицински изделия съгласно определението в член 2, точка 1 от Регламент (ЕС) 2017/745, и субекти, произвеждащи медицински изделия за инвитро диагностика съгласно определението в член 2, точка 2 от Регламент (ЕС) 2017/746, с изключение на субектите, произвеждащи медицински изделия съгласно определението в приложение I, точка 5, пето тире от директива МИС 2

б) Производство на компютри, електронни и оптични продукти

Предприятия, извършващи някоя от икономическите дейности съгласно определението в раздел B, разделение 26 на NACE Rev. 2 – според -Закон за административното регулиране на производството на оптични дискове и матрици

в) Производство на електрически съоръжения

Предприятия, извършващи някоя от икономическите дейности съгласно определението в раздел B, разделение 27 на NACE Rev. 2 - сектор Производство на електрически съоръжения (код 27 по КИД-2008)

20. Доставчици на цифрови услуги;
21. Научни изследвания;

1.2. Засегнати органи за надзор и държавни органи според въведените нови сектори:

1. Министерство електронното управление - в качеството му на компетентен орган за надзор над дейността на административните органи;
2. Министерство на енергетиката;
3. Министерство на транспорта и съобщенията;
4. Комисията за регулиране на съобщенията;
5. Министерство на здравеопазването;
6. Министерство на регионалното развитие и благоустройството;
7. Български пощи;

Посочете всички потенциални заинтересовани страни/групи заинтересовани страни (в рамките на процеса по извършване на частичната предварителна частична оценка на въздействието и/или при обществените консултации по чл. 26 от Закона за нормативните актове), върху които предложенията ще окажат пряко или косвено въздействие (бизнес в дадена област/всички предприемачи, неправителствени организации, граждани/техни представители, държавни органи/общини и др.).

4. Варианти на действие. Анализ на въздействията:

4.1. По проблем 1: Необходимост от транспониране на Директива(ЕС) 2022/2555 (Директива МИС2) поради *непълно съответствие на действащата нормативна уредба, липса на съгласуваност с действащите разпоредби в тази област на политиката.*

Вариант 1 „Без действие“:

Описание:

При този вариант няма да бъдат предприети никакви действия за осигуряване на необходимите условия за привеждане на националното законодателство в съответствие с изискванията на европейската правна рамка, респективно няма да бъдат регламентирани и действия за въвеждане на изискванията на директива (ЕС) 2022/2555.

Рискове: Изборът на този вариант би означавал неизпълнение от страна на България на задълженията, произтичащи от законодателството на ЕС, което създава риск от предприемане на правни действия срещу страната, съгласно член 258 от ДФЕС. Законът за киберсигурност ще има ограничено приложение. При този вариант Европейската комисия ще стартира наказателна процедура за нарушение срещу Република България.

Положителни (икономически/социални/екологични) въздействия: Не се наблюдават.

Отрицателни (икономически/социални/екологични) въздействия: Не се наблюдават.

Специфични въздействия: Не се наблюдават.

Въздействия върху малките и средните предприятия: Не се наблюдават.

Административна тежест: Не се наблюдават.

Вариант 2 „Максимално широк обхват и стриктна регулация“:

Описание:

Този вариант изисква значително разширяване на кръга обществени отношения, включени в минималния обхват на Директивата, което означава стриктни регулации и минимална възможност

за адаптиране на рамката към последващи изменения или развитие в тях. В обобщен вариант регулацията ще обхване следните групи мерки:

При този вариант се предвижда в националното законодателство да се въведе цялостна уредба относно изискванията за киберсигурност и условия за управление и противодействие на рисковете касаещи съществените и важни субекти, както и отговарящите на зададените критерии, попадащи в определените сектори в Приложение 1 и 2,; на компетентните органи се предоставят широки пълномощия по управление и надзор политиките по киберсигурност по отношение определените субекти – съществени и важни; компетентните органи следва да бъдат оправомощени да прилагат санкции, състоящи се в спиране на сертифициране или разрешение относно част или всички услуги пропорционално на тежестта на нарушението, само като ultima ratio, което означава само след изчерпване на другите съответни действия по прилагане, за времето, докато субектите, спрямо които се прилагат, предприемат необходимите действия за отстраняване на недостатъците; след установен минимален списък на административните санкции за нарушаване на задълженията за управление на риска от киберсигурност и докладване, се създава ясна и последователна рамка за санкциите, според естеството, тежестта и продължителността на нарушението, действителните причинени вреди или нанесените загуби или потенциални щети или загуби, които биха могли да бъдат предизвикани, умишлен или небрежен характер на нарушението, действията, предприети за предотвратяване или смекчаване на претърпени вреди и/или загуби, степента на отговорност или съответните предишни нарушения, степента на сътрудничество с компетентния орган и всеки друг утежняващ или смекчаващ фактор. Всеки компетентен орган следва да има правомощието да налага административни глоби; да се създаде система, която предвижда ефективни, пропорционални и възпиращи санкции. Естеството на такива наказания, наказателни или административни, се определя в ЗИД на ЗКС; като допълнение ще се насърчи обменът на данни за заплахите, спазването на мерките за управление на риска в областта на киберсигурността и задълженията за докладване и т.н.

Рискове:

При избора на „максимално широк обхват“ и едновременно на стриктна регулация, създава рискове за значително ограничаване на възможностите за адаптиране на законовата рамка към последващи изменения или развитие, за осигуряване на гъвкави способи за регулация и ефективна оценка по целесъобразност на всички предприети мерки; въвеждането на всеобхватен и лимитиран режим няма да осигури, а ще затрудни свободата на самоопределянето всички субекти, ще затрудни адаптирането на новите сектори към съществуващите правила и изисквания, като същевременно няма да бъде направена необходимата цялостна и подробна оценка на въздействието по отношение на всички субекти – съществени и важни, както и определените по различен критерии лица, попадащи под регулацията на посочените обществени отношения.

Това би довело до обратен ефект, на търсения в уредбата на Директивата.

Положителни (икономически/социални/екологични) въздействия:

- Ще се осигури пълното транспониране на Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета;
- Ще се подобрят и оптимизират процесите по регулация на киберсигурността в Р България;
- Ще се разшири обхвата на ЗКС с ново-присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на националните компетентни органи;
- Ще се усъвършенства режимът за реализация на отговорността на субектите на ЗКС и ще се повиши степента на подготвеност на съществените и важни субекти в областта на киберсигурността, което от своя страна ще смекчи потенциалните загуби на приходи поради кибератаки

- Ще се усъвършенства координираният подход в изграждането на способности за киберсигурност в Р България и смекчаване на заплахите за мрежовата и информационна сигурност.

Отрицателни (икономически/социални/екологични) въздействия: Не се наблюдават.

Специфични въздействия: Не се наблюдават.

Въздействия върху малките и средните предприятия: Проектозаконът ще се прилага по отношение на някои публичноправни или частноправни съществени субекти, упражняващи дейност в изброените в Приложение I сектори (енергетика; транспорт; банково дело; инфраструктури на финансовия пазар; здравеопазване, питейна вода; отпадъчни води; цифрова инфраструктура; публична администрация и космическо пространство), както и на някои важни субекти, упражняващи дейност в изброените в Приложение II сектори (пощенски и куриерски услуги; управление на отпадъците; производство на изделия и вещества и дистрибуция на химикали; производство, преработка и разпространение на храни; производствени и цифрови доставчици). Микропредприятията и малките предприятия по смисъла на Препоръка 2003/361/ЕО на Комисията от 6 май 2003 г. са изключени от обхвата на директивата, с изключение на доставчиците на електронни съобщителни мрежи или на общественодостъпни електронни съобщителни услуги, доставчиците на удостоверителни услуги, регистрите на имената на домейни от първо ниво (TLD) и публичната администрация, както и на някои други субекти, като например единствени доставчици на дадена услуга в дадена държава членка. Предприятията могат да варират, доколкото се променят индикаторите за оценка на „съществен“ или „важен“ субект се идентифицират спрямо ЗМСП, като за част от тях могат да отпаднат, или да се добавят други заинтересовани страни. Всички потенциално 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.) се посочват по сектори, по нормативна определеност и прилежание към даден бранш.

Административна тежест: Разширяването на обхвата на закона, с добавянето на нови сектори, съответно разширява и кръга на субектите имащи задължения за докладване на инциденти, но то не е съпроводено с изменение на процедурите по докладване.

Вариант 3 „*Балансиран подход*“:

Описание: При този вариант се постига максимален баланс между заложените в Директивата

цели и националните приоритети. Държавата се възползва само от текстовете, които допринасят за екзактното транспониране на Директива (ЕС) 2022/2555 в националното законодателство, при гарантиране на еднакво и обективно прилагане и надграждане на съществуващите правила и запълване на непълнотите. Този подход осигурява максимална адаптивност на новите изисквания със съществуващите текстове в ЗКС, по-голяма оперативност, възможност за по–ефективно надграждане на досега определените и новосъздадените субекти, попадащи под регулацията на Директивата. Описаните рискове при „Максимално широк обхват и стриктна регулация“ ще бъдат избегнати и облекчени до степен да се избегне хипер регулация водеща до неефективност на прилагането от националните компетентни отгани и ЕРИКС-и. Цели се запазване на адаптивността на рамка по транспониране на директивата дори при нарастване на регулираните субекти.

Рискове: При избора на балансиран подход за транспониране на Директивата, ще се избегнат посочените рискове във Вариант 2, ще се запази досега съществуващата определеност на органите в Република България, ще бъдат разширени техните правомощия до степен, която няма да въведе хипер регулация, а ще бъде съобразена с конституентите на закона в страната и новите сектори след разширяването на обхвата, но същевременно балансирана и съобразена с целите на европейското правоприлагане.

Ще бъде предвиден ефективен надзор върху съществените и важни субекти, като същевременно се предвижда създаването на механизми за административното им подпомагане, изключването на свръх-регулация, поради създаването и на евентуална административна тежест.

Положителни (икономически/социални/екологични) въздействия:

Социални въздействия:

- Основните социални въздействия ще попаднат върху съществените и важни субекти. За да предотвратят негативните последици от засягането на мрежите и информационните си системи и да се предпазят от неправомерни посегателства и инциденти, които могат да предизвикат тежки преки и непреки последици за обективното икономическо и финансово състояние на всеки, субектите ще въведат стандартизиран набор от правила и процедури за управление на рисковете и ще бъдат насърчени да инвестират в технологични решения, за да осигурят по-високи нива на киберсигурност, като по този начин се подобри цялостната устойчивост на сектора към който принадлежат. Очакванията са постигане на по-високите нива на киберсигурност, намаляване и ограничаване на броя на инцидентите. Повишаването на киберсигурността в все повече сектори на икономиката неизменно означава и положителен резултат, по-висока защита на обществото.

Екологични въздействия:

Потреблението на енергия от електрически уреди, по-специално от устройства, използвани от или подпомагащи ИКТ и други енергоемки технологии, нараства. Поради това е важно да се насърчи приемането на технологии с ниски емисии в съответствие с целите, определени в съобщението на Комисията относно Европейския зелен пакт и Индустриалната стратегия на Комисията.

С въвеждането на мерки по прилагането на регламента се очаква насърчаването на засиленото използване на ИКТ инфраструктури и услуги от последно поколение, които са по-устойчиви от гледна точка на околната среда. С осигуряване на правна яснота относно споразуменията с трети страни доставчици на услуги в областта на ИКТ се очаква увеличаване на използването им. Третите страни, доставчици на услуги в областта на ИКТ, като цяло са по-енергийно ефективни от вътрешната ИКТ инфраструктура. По-високите нива на ефективност на последните технологии и инфраструктури за сигурност ще допринесат за намаляване на потреблението на електричество, вода и други течности, използвани за охлаждане на центрове за данни, като по този начин ще имат положително въздействие върху околната среда чрез намаляване на вредните емисии. Новите и интелигентни технологии също са изградени с екологични материали, които ще улеснят рециклирането след приключване на жизнения им цикъл.

- Ще се осигури оптималност на транспонираните текстове на Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета, като ще са в ясна корелация със съществуващите текстове на ЗКС;
- Ще се подобрят и оптимизират процесите по регулация на киберсигурността в Р България;
- Ще се разшири обхвата на ЗКС с ново-присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на националните компетентни органи;
- Ще се усъвършенства режимът за реализация на отговорността на субектите на ЗКС и ще се повиши степента на подготвеност на съществените и важни субекти в областта на киберсигурността, което от своя страна ще смекчи потенциалните загуби на приходи поради кибератаки;

Отрицателни (икономически/социални/екологични) въздействия: Не се наблюдават.

Специфични въздействия: Не се наблюдават.

Въздействия върху малките и средните предприятия: Проектозаконът ще се прилага по отношение на някои публичноправни или частноправни съществени субекти, упражняващи дейност в изброените в Приложение I сектори (енергетика; транспорт; банково дело; инфраструктури на финансовия пазар; здравеопазване, питейна вода; отпадъчни води; цифрова инфраструктура; публична администрация и космическо пространство), както и на някои важни субекти, упражняващи дейност в изброените в Приложение II сектори (пощенски и куриерски услуги; управление на отпадъците; производство на изделия и вещества и дистрибуция на химикали; производство, преработка и разпространение на храни; производствени и цифрови доставчици). Мерките за високо общо ниво на киберсигурност са организационни, технологични и технически и се прилагат в съответствие със спецификата на субектите и пропорционално на заплахите с цел минимизиране на риска от тяхното реализиране, казва регулацията. По отношение на микропредприятията и малките предприятия по смисъла на Препоръка 2003/361/ЕО на Комисията от 6 май 2003 г. са изключени от обхвата на директивата, с изключение на доставчиците на електронни съобщителни мрежи или на общественодостъпни електронни съобщителни услуги, доставчиците на удостоверителни услуги регистрите на имената на домейни от първо ниво (TLD) и публичната администрация, както и на някои други субекти, като например единствени доставчици на дадена услуга в дадена държава членка. Предприятията могат да варират, доколкото се променят индикаторите за оценка на „съществен“ или „важен“ субект се идентифицират спрямо ЗМСП, като за част от тях могат да отпаднат, или да се добавят други заинтересовани страни. Всички потенциално 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.) се посочват по сектори, по нормативна определеност и прилежание към даден бранш.

Административна тежест: Разширяването на обхвата на закона, с добавянето на нови сектори, съответно разширява и кръга на субектите имащи задължения за докладване на инциденти, но то не е съпроводено с изменение на процедурите по докладване. Предвид създаването на по-високи изисквания в действащото законодателство за осъществяване на надзор по отношение на дейността на по-голям кръг икономически субекти, както и на отсъствието на част от предвидените в Директивата правни институти и задължения от сега действащия режим, новата уредба неизбежно ще доведе до повишаване на административната тежест върху заинтересованите лица. Създаване на нови регулаторни режими и въздействие върху съществуващи режими. Новата уредба има за цел да разшири обхвата на субектите попадащи под регулацията на проектозакона, като установи повече и по-високи изисквания, по отношение на които компетентният орган осъществява предварителен и последващ надзор. В този режим на надзорните органи ще бъдат предоставени редица надзорни и санкционни правомощия, в т.ч. правото да издава принудителни административни мерки.

Разходите във връзка с докладването на инциденти например, ще зависи до голяма степен от пропорционалността на бъдещите правила и установяването на праговете на същественост, които ще предизвикат докладване (напр. съществени инциденти).

По отношение на **третите страни, доставчици на услуги в областта на ИКТ,** разходите ще са свързани с организационни промени, за да позволят надзора на техните дейности.

По отношение на **надзорните органи** може да се очаква увеличение на разходите във връзка с допълнителните правомощия, които надзорните органи ще осъществяват (напр. допълнително докладване на инциденти). Надзорните органи, които биха участвали в прекия надзор на трети страни, доставчици на услуги **в областта на ИКТ,** (напр. споразумения за сътрудничество, съвместни инспекции и обмен на информация), се очаква да имат по-големи разходи.

4.2. По проблем 2: Необходимостта от изграждане на координиран подход относно Директива (ЕС) 2022/2555, насочена към изграждане на способности за киберсигурност в целия Съюз,

смекчаване на заплахите за сигурността на мрежите и информационните системи, използвани за предоставяне на основни услуги в ключови сектори, и осигуряване на приемственост на такива услуги при изправяне пред тях инциденти с киберсигурност, като по този начин допринася за ефективната икономика и общество на Съюза.

Вариант 1 „Без действие“:

Описание:

При този вариант няма да бъдат предприети никакви действия за осигуряване на координиран подход и за привеждане на националното законодателство в съответствие с изискванията на европейската правна рамка, респективно няма да бъдат регламентирани и действия за въвеждане на изискванията на директива (ЕС) 2022/2555.

Рискове: Изборът на този вариант би означавал неизпълнение от страна на България на задълженията, произтичащи от законодателството на ЕС, което създава риск от предприемане на правни действия срещу страната, съгласно член 258 от ДФЕС. Законът за киберсигурност ще има ограничено приложение. При този вариант Европейската комисия ще стартира наказателна процедура за нарушение срещу Република България.

Положителни (икономически/социални/екологични) въздействия: Не се наблюдават.

Отрицателни (икономически/социални/екологични) въздействия: Не се наблюдават.

Специфични въздействия: Не се наблюдават.

Въздействия върху малките и средните предприятия: Не се наблюдават**.**

Административна тежест: Не се наблюдават**.**

Вариант 2 „Максимално широк обхват и стриктна регулация“:

Описание:

Този вариант изисква да се разшири обхватът на закона, което означава стриктни регулации и минимална възможност за адаптиране на рамката към последващи изменения или развитие в тях. В обобщен вариант регулацията ще обхване следните групи мерки:

- Предвижда се въвеждане в цялостната нормативна уредба на значителна промяна в съществуващите до момента практики и процеси, установяване и преразглеждане на национални способности, органи и институции, а и прилагане на нови регулаторни мерки, обхващащи основни инфраструктури относно изискванията за киберсигурност и условия за управление и противодействие на рисковете касаещи съществените и важни субекти, както и отговарящите на зададените критерии, попадащи в определените сектори в Приложение 1 и 2;
- На компетентните органи се предоставят широки пълномощия по управление и надзор политиките по киберсигурност по отношение определените субекти – съществени и важни.
- Изискването за осъществяване на доброволно сътрудничество между отговорните институции, мерките за общо прилагане и взаимодействие да бъдат подсилени, както и от гледна точка на правоприлагането на национално ниво, ще гарантира подсигурен координиран подход и насочена към изграждане на способности киберсигурност в целия Съюз, както и смекчаване на заплахите. Изграждането на координационен ЕРИКС, който да изпълнява функциите по Директивата, обмена на служители, както на национално, така и на европейско ниво, обединяването на взаимодействието между EU-CyCLONe и мрежата CSIRTs, определянето на повече от един НКО, отговорен за изпълнението на задачите, свързани със сигурността на МИС на съществени и важни субекти съгласно директивата, широкото сътрудничество с академични и изследователски институции, въвеждането на механизъм за партньорски проверки, позволяващ оценка от експерти, определени от държавите-членки, на прилагането на политиките за киберсигурност, включително нивото на способностите на държавите-членки и наличните ресурси и др. са мерки които изискват наличие на заявен политически модел на

взаимодействие, координиран подход на една развита и работеща в пълен обем национална кибер система.
- Създаването на правила за сътрудничество между компетентните органи и надзорните органи в съответствие с Регламент (ЕС) 2016/679 за справяне с нарушения, свързани с лични данни, както и осигуряването на високо ниво на отговорност за мерките за управление на риска в киберсигурността и задълженията за докладване на ниво организации, субектите следва да одобрят мерките за кибер риск от и да контролират тяхното прилагане, също и управлението на риска, сертификацията по специфични европейски схеми за сертифициране на киберсигурността.

Рискове:

При избора на „максимално широк обхват“ и едновременно на стриктна регулация, се създават рискове за значително ограничаване на възможностите за адаптиране на законовата рамка; въвеждането на всеобхватен и лимитиран режим няма да осигури, а ще затрудни свободата на самоопределянето всички субекти, ще затрудни адаптирането на новите сектори към съществуващите правила и изисквания, напр.

Административнонаказателен орган, който да гарантира:

- ефективно наблюдение;
- да следи за изпълнението и предприемането на необходимите мерки, за спазването на правилата, които са ефективни, пропорционални и възпиращи, като се вземат предвид обстоятелствата за всеки отделен случай,
- чрез проверки на място и надзор извън обекта, включително произволни проверки;
- редовни одити; целенасочени одити на сигурността въз основа на оценки на риска или свързана с риска налична информация;
- сканиране за сигурност, основаващо се на обективни, недискриминационни, справедливи и прозрачни критерии за оценка на риска;
- искания за информация, необходима за оценка на мерките за киберсигурност, приети от субектите,
- включително документирани политики за киберсигурност, както и
- спазването на задължението за уведомяване на ENISA съгласно член 25, параграфи 1 и 2;
- искания за достъп до данни, документи или каквато и да е информация, необходима за изпълнението на техните надзорни задачи; искания за доказателства за прилагане на политики за киберсигурност, като например резултатите от одитите за сигурност, извършени от квалифициран одитор, и съответните основни доказателства.

При „Максимално широк обхват и стриктна регулация“, няма да бъде направена необходимата цялостна и подробна оценка на въздействието по отношение на всички субекти - съществени и важни, както и определените по различен критерии лица, попадащи под регулацията на посочените обществени отношения.

Това би довело до обратен ефект, на търсения в уредбата на Директивата.

Положителни (икономически/социални/екологични) въздействия:

- Ще се усъвършенства координираният подход в изграждането на способности за киберсигурност в Р България и смекчаване на заплахите за мрежовата и информационна сигурност.
- Ще се осигури пълното транспониране на Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета чрез значителна промяна в съществуващите до момента практики и процеси;
- Ще се оптимизират процесите по регулация на киберсигурността в Р България;
- Ще се разшири обхвата на ЗКС с ново-присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на националните компетентни органи;

- Ще се усъвършенства режимът за реализация на отговорността на субектите на ЗКС и ще се повиши степента на подготвеност на съществените и важни субекти в областта на киберсигурността, което от своя страна ще смекчи потенциалните загуби на приходи поради кибератаки

Отрицателни (икономически/социални/екологични) въздействия: Не се наблюдават.

Специфични въздействия: Не се наблюдават.

Въздействия върху малките и средните предприятия: Възприемането на максимална регулация при координирания подход засяга в голяма степен разпределението на ролите и отговорностите в сектор държавна администрация, като отражението му в МСП може да варира, доколкото се променят индикаторите за оценка на „съществен“ или „важен“ субект се идентифицират спрямо ЗМСП, като за част от тях могат да отпаднат, или да се добавят други заинтересовани страни. Всички потенциално 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.) се посочват по сектори, по нормативна определеност и прилежание към даден бранш.

Административна тежест: Разширяването на обема от задължения за административните органи за осигуряване на координирания подход, изграждане и надграждане на съществуващи способности в държавната администрация.

Вариант 3 „Балансиран подход“:

Описание: При този вариант се постига максимален баланс между заложените в Директивата цели и националните приоритети. Държавата се възползва само от текстовете, които допринасят за екзактното транспониране на Директива (ЕС) 2022/2555 в националното законодателство, при гарантиране на еднакво и обективно прилагане и надграждане на съществуващите правила и запълване на непълнотите. Този подход осигурява максимална адаптивност на новите изисквания със съществуващите текстове в ЗКС, по -голяма оперативност, възможност за по – ефективно надграждане на досега – определените и новосъздадените субекти, попадащи под регулацията на Директивата. Описаните рискове при „Максимално широк обхват и стриктна регулация“ ще бъдат избегнати и облекчени до степен да се избегне хипер-регулация водеща до неефективност на прилагането от националните компетентни органи и ЕРИКС-и. Цели се запазване на адаптивността на рамка по транспониране на директивата дори при нарастване на регулираните субекти.

Рискове: При избора на балансиран подход за транспониране на Директивата, ще се избегнат посочените рискове във Вариант 2, ще се запази досега съществуващата определеност на органите в Република България, ще бъдат разширени техните правомощия до степен, която няма да въведе хипер регулация, а ще бъде съобразена с конституентите на закона в страната и новите сектори след разширяването на обхвата, но същевременно балансирана и съобразена с целите на европейското правоприлагане.

Ще бъде предвиден ефективен надзор върху съществените и важни субекти, като същевременно се предвижда създаването на механизми за административното им подпомагане, изключването на свръх-регулация, поради създаването и на евентуална административна тежест.

Положителни (икономически/социални/екологични) въздействия:

Социални въздействия:

-Попадат върху административните органи. Не се предвижда създаване на финансова тежест за обществото.

Екологични въздействия:

- Потреблението на енергия от електрически уреди, по-специално от устройства, използвани от или подпомагащи ИКТ и други енергоемки технологии, нараства. Поради това е важно да се насърчи приемането на технологии с ниски емисии в съответствие с целите, определени в съобщението на Комисията относно Европейския зелен пакт и Индустриалната стратегия на Комисията.

С въвеждането на мерки по прилагането на директивата се очаква насърчаването на засиленото използване на ИКТ инфраструктури и услуги от последно поколение, които са по-устойчиви от гледна точка на околната среда. С осигуряване на правна яснота относно споразуменията с трети страни доставчици на услуги в областта на ИКТ се очаква увеличаване на използването им. Третите страни доставчици на услуги в областта на ИКТ като цяло са по-енергийно ефективни от вътрешната ИКТ инфраструктура. По-високите нива на ефективност на последните технологии и инфраструктури за сигурност ще допринесат за намаляване на потреблението на електричество, вода и други течности, използвани за охлаждане на центрове за данни, като по този начин ще имат положително въздействие върху околната среда чрез намаляване на вредните емисии. Новите и интелигентни технологии също са изградени с екологични материали, които ще улеснят рециклирането след приключване на жизнения им цикъл.

- Ще се осигури оптималност на транспонираните текстове на Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета, като ще са в ясна корелация със съществуващите текстове на ЗКС;
- Ще се подобрят и оптимизират процесите по регулация на киберсигурността в Р България;
- Ще се разшири обхвата на ЗКС с ново-присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на националните компетентни органи;
- Ще се усъвършенства режимът за реализация на отговорността на субектите на ЗКС и ще се повиши степента на подготвеност на съществените и важни субекти в областта на киберсигурността, което от своя страна ще смекчи потенциалните загуби на приходи поради кибератаки;

Отрицателни (икономически/социални/екологични) въздействия: Не се наблюдават.

Специфични въздействия: Не се наблюдават.

Въздействия върху малките и средните предприятия: Разширяването на обхвата на закона, с добавянето на нови сектори, съответно разширява и кръга на субектите имащи задължения за докладване на инциденти, но то не е съпроводено с изменение на процедурите по докладване.

Административна тежест: Възприемането на балансираният подход в регулацията ще позволи на разгръщането и надграждането на съществуващият модел на взаимодействие между институциите в Република България. Ще доведе до плавно и поетапно изграждане на по-стабилно взаимодействие и разпределение на отговорностите както на ниво междуведомствени оперативни действия, така и в ескалационен план, достигайки политическо ниво при вземане на решения по отношение на европейски и трансграничен инцидент например.

4.3. По проблем 3: ***Допълване на основни сегменти, както и разширяване на икономическите сектори по Директива (ЕС) 2022/2555, осъществяване на регулацията им посредством надграждане дейността и добавяне на правомощия на националните компетентни органи***

Вариант 1 „Без действие“:

Описание:

При този вариант няма да бъдат предприети никакви действия за разширяване обхвата на секторите и за привеждане на националното законодателство в съответствие с изискванията на европейската правна рамка, респективно няма да бъдат регламентирани и действия за въвеждане регулацията за новите сектори на директива (ЕС) 2022/2555.

Рискове: Изборът на този вариант би означавал неизпълнение от страна на България на задълженията, произтичащи от законодателството на ЕС, което създава риск от предприемане на правни действия срещу страната, съгласно член 258 от ДФЕС. Законът за киберсигурност ще има ограничено приложение. При този вариант Европейската комисия ще стартира наказателна процедура за нарушение срещу Република България.

Положителни (икономически/социални/екологични) въздействия: Не се наблюдават.

Отрицателни (икономически/социални/екологични) въздействия: Не се наблюдават.

Специфични въздействия: Не се наблюдават.

Въздействия върху малките и средните предприятия: Не се наблюдават.

Административна тежест: Не се наблюдават**.**

Вариант 2 „Максимално широк обхват и стриктна регулация“:

Описание: Този вариант изисква да се разшири обхвата на закона, което означава стриктни регулации и минимална възможност за адаптиране на рамката. В обобщен вариант регулацията ще обхване следните групи мерки:

- Нови регулаторни мерки, обхващащи основни инфраструктури относно изискванията за киберсигурност и условия за управление и противодействие на рисковете касаещи съществените и важни субекти, както и отговарящите на зададените критерии, попадащи в определените сектори в Приложение 1 и 2;

Управителните органи на субектите, попадащи в обхвата, следва да прилагат мерките за риск от киберсигурност и да контролират изпълнението им, също и управлението на риска, сертификацията по специфични европейски схеми за сертифициране на киберсигурността, но най – изявената и трудоемка промяна за имплементиране се състои в обособяването на Административнонаказателен орган, които да гарантира:

- ефективно наблюдение;
- да следи за изпълнението и предприемането на необходимите мерки, за спазването на правилата, които са ефективни, пропорционални и възпиращи, като се вземат предвид обстоятелствата за всеки отделен случай:
    - чрез проверки на място и надзор извън обекта, включително произволни проверки;
    - редовни одити; целенасочени одити на сигурността въз основа на оценки на риска или свързана с риска налична информация;
    - сканиране за сигурност, основаващо се на обективни, недискриминационни, справедливи и прозрачни критерии за оценка на риска;
    - искания за информация, необходима за оценка на мерките за киберсигурност, приети от субектите,
    - включително документирани политики за киберсигурност, както и
    - спазването на задължението за уведомяване на ENISA съгласно член 25, параграфи 1 и 2;
    - искания за достъп до данни, документи или каквато и да е информация, необходима за изпълнението на техните надзорни задачи; искания за доказателства за прилагане на политики за киберсигурност, като например резултатите от одитите за сигурност, извършени от квалифициран одитор, и съответните основни доказателства.

Всичко това определя важността на транспонирането на национално ниво Директивата и необходимостта на новосъздадените правила да залегнат дългосрочно в законодателството на киберсигурността на страната.

В основата си транспонирането на Директива заляга върху възможността за продължаване на някои съществуващи практики, за надграждане на други основни сегменти, както и допълване и разширяване на икономически сектори. Но не трябва да се забравя, че секторите и към настоящия

момент в закона не са малко, допълването има на практика с 2 нови подсектора и 10 изцяло нови сектора, ще разшири обхвата, но на практика няма да промени основно и сега съществуващите браншове и сектори в страната.

Рискове: Създаването на надзорния орган ще създаде тежест и за бизнеса и за администрацията. Санкционните режими без подходяща адаптация на нормативните текстове ще трябва също да предвиждат възможността за суспендиране на правомощия изграждат един изцяло нов и утежнен административен процес. Вменяването на нови и широки правомощия у наказателните органи ще доведе до забавяне процесите по имплементация на мерките за киберзащита и ще увеличи рисковете за бизнеса и икономиката. А гарантирането на ефективността им ще бъде дълъг и трудоемък процес. Предприемането на необходимите действия за отстраняване на недостатъците в определения срок, преустановяване сертифицирането или разрешението налагат или изискват налагането от съответните органи или съдилища съгласно националното законодателство на временни забрани срещу субектите, а определянето на действителните причинени вреди или претърпени загуби или потенциални щети или загуби, които биха могли да бъдат предизвикани, изисква сериозна експертиза и административен опит в киберсигурността или МИС.

Положителни (икономически/социални/екологични) въздействия:

- Ще се увеличи значително обхватът на закона за киберсигурност;
- Ще се осигури пълното транспониране на Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета чрез значителна промяна в съществуващите до момента субекти по ЗКС;
- Ще се оптимизират секторите на киберсигурността в Р България;
- Ще се разшири обхвата на ЗКС с ново-присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на националните компетентни органи;

Отрицателни (икономически/социални/екологични) въздействия: Не се наблюдават.

Специфични въздействия: Не се наблюдават.

Въздействия върху малките и средните предприятия: Възприемането на максимална регулация при координирания подход засяга в голяма степен разпределението на ролите и отговорностите в сектор държавна администрация, като отражението му в МСП може да варира, доколкото се променят индикаторите за оценка на „съществен“ или „важен“ субект се идентифицират спрямо ЗМСП, като за част от тях могат да отпаднат, или да се добавят други заинтересовани страни. Всички потенциално 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.) се посочват по сектори, по нормативна определеност и прилежание към даден бранш.

Административна тежест: При избора на „максимално широк обхват“ и едновременно на стриктна регулация, се създават рискове за значително ограничаване на възможностите за адаптиране на законовата рамка; въвеждането на всеобхватен и лимитиран режим няма да осигури, а ще затрудни свободата на самоопределянето всички субекти, ще затрудни адаптирането на новите сектори към съществуващите правила и изисквания, напр.:

При „Максимално широк обхват и стриктна регулация“, няма да бъде направена необходимата цялостна и подробна оценка на въздействието по отношение на всички субекти –съществени и важни, както и определените по различен критерии лица, попадащи под регулацията на посочените обществени отношения.

Разширяването на обема от задължения за административните органи за осигуряване на координирания подход, изграждане и надграждане на съществуващи способности в държавната администрация.

Вариант 3 „Балансиран подход“:

Описание: При този вариант се постига максимален баланс между заложените в Директивата цели и националните приоритети. Държавата се възползва само от текстовете, които допринасят за екзактното транспониране на Директива (ЕС) 2022/2555 в националното законодателство, при гарантиране на еднакво и обективно прилагане и надграждане на съществуващите правила и запълване на непълнотите. Този подход осигурява максимална адаптивност на новите изисквания със съществуващите текстове в ЗКС, по -голяма оперативност, възможност за по – ефективно надграждане на досега – определените и новосъздадените субекти, попадащи под регулацията на Директивата. Описаните рискове при „Максимално широк обхват и стриктна регулация“ ще бъдат избегнати и облекчени до степен да се избегне хипер-регулация водеща до неефективност на прилагането от националните компетрнтни отгани и ЕРИКС-и. Цели се запазване на адаптивността на рамка по транспониране на директивата дори при нарастване на регулираните субекти.

Рискове: При избора на балансиран подход за транспониране на Директивата, ще се избегнат посочените рискове във Вариант 2, ще се надгради досега съществуващата рамка на конституентите, субектите попадащи в обхвата на ЗКС в Република България, като разширяването на обхвата, ще бъде същевременно балансирано и съобразена с целите на европейското правоприлагане.

Положителни (икономически/социални/екологични) въздействия:

Социални въздействия:

- Ще се подобрят и оптимизират процесите по регулация на киберсигурността в Р България;
- Ще се разшири обхвата на ЗКС с ново-присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на националните компетентни органи;
- Ще се предприемат мерки за прецизиране на нормативната уредба и създаване на ясен и ефективен режим, който да регулира задълженията на съществените и важни субекти в съответствие с въведените в директивата по – високи изисквания при постигане на киберсигурността на субектите, при запазване на изискванията за защита на мрежите и информационните системи. В ЗИД на ЗКС са предвидени общи цели по отношение на дейността по отношение на ново-обхванатите сектори, главно поради:

1.повишената цифровизация през последните години и по-високата степен на взаимосвързаност,

2. факта, че понастоящем съществуващият обхват вече не отразява всички цифровизирани сектори, предоставящи ключови услуги за икономиката и обществото като цяло. Поради което в икономически план ще настъпят следните благоприятни изменения:

- обхвата на операторите на основни услуги, ще бъде изяснен в достатъчна степен с оглед на доставчиците на цифрови услуги, идентифицирани като такива във всички държави членки, с цел да въвеждат мерки за сигурност и да докладват за инциденти;
- ще се уеднакви определянето на изискванията за сигурност и докладването на инциденти;
- ще се балансира режимът на надзор и правоприлагане, налагане на санкции на субекти, които не са въвели изискванията за сигурност или не са докладвали за инциденти;
- Ще се надгради систематичният обмен на информация с цел подобряване на ефективността на мерките за киберсигурност и за степента на съвместна ситуационна осведоменост на равнището на ЕС. Случаят е такъв и при обмена на информация между частноправни субекти, както и при обмена между структурите за сътрудничество на равнището на ЕС и частноправните субекти.

Екологични въздействия: Не се очаква Вариант 3 да окаже влияние върху измененията на климата, транспорта и използването на енергия, биоразнообразието, чистотата на атмосферния въздух, качеството на водите и водните запаси, качеството на почвата, възобновяемите или

невъзобновяемите ресурси, фирмите и потребителите върху околната среда отпадъци/генериране/рециклиране, предвид отношенията, които се регулират със законопроекта.

Отрицателни (икономически/социални/екологични) въздействия: Не се наблюдават.

Специфични въздействия: Не се наблюдават.

Въздействия върху малките и средните предприятия: Разширяването на обхвата на закона, с добавянето на нови сектори, съответно разширява и кръга на субектите имащи задължения за докладване на инциденти, но то не е съпроводено с изменение на процедурите по докладване.

Административна тежест: Възприемането на балансираният подход в регулацията при допълване на основни сегменти, както и разширяване на икономическите сектори ще позволи на разгръщането и надграждането на съществуващият обхват, който вече не отразява всички цифровизирани сектори, предоставящи ключови услуги за икономиката и обществото като цяло.

5. Сравняване на вариантите:

Степени на изпълнение по критерии: 1) висока; 2) средна; 3) ниска.

5.1. По проблем 1: *Непълно съответствие на действащата нормативна уредба, липса на съгласуваност с действащите разпоредби в тази област на политиката.*

		Вариант 1 „Без действие“	**Вариант 2 Максимално широк обхват и стриктна регулация“**	**Вариант 3 „Балансиран подход”**
Ефективност	**Цел 1:** *Повишаване на степента на подготвеност на съществените и важни субекти в областта на киберсигурността би довело до смекчаване на потенциалните загуби на приходи поради кибератаки и би намалило големите разходи за смекчаване на заплахите ad-hoc.*	3	2	1
	Цел 2: *Допълване и усъвършенстване на съществуващия нормативен режим за съществените и важни субекти в съответствие с изискванията на Директива (ЕС)2022/2555*	3	2	1
	Цел 3: *Адаптиране на съществуващата нормативна рамка в ЗКС в съответствие с изискванията на Директива (ЕС) 2022/2555, както и разширяване на компетенциите на компетентните органи по киберсигурност в Р България*	3	2	1
	Цел 4: *Регулация на присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на Националните компетентни органи*	3	2	1

Ефикасност	**Цел 1:** *Повишаване на степента на подготвеност на съществените и важни субекти в областта на киберсигурността би довело до смекчаване на потенциалните загуби на приходи поради кибератаки и би намалило големите разходи за смекчаване на заплахите ad-hoc.*	3	2	1
	Цел 2: *Допълване и усъвършенстване на съществуващия нормативен режим за съществените и важни субекти в съответствие с изискванията на Директива (ЕС)2022/2555*	3	2	1
	Цел 3: *Адаптиране на съществуващата нормативна рамка в ЗКС в съответствие с изискванията на Директива (ЕС) 2022/2555, както и разширяване на компетенциите на компетентните органи по киберсигурност в Р България*	3	2	1
	Цел 4: *Регулация на присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на Националните компетентни органи*	3	2	1
Съгласуваност	**Цел 1:** *Повишаване на степента на подготвеност на съществените и важни субекти в областта на киберсигурността би довело до смекчаване на потенциалните загуби на приходи поради кибератаки и би намалило големите разходи за смекчаване на заплахите ad-hoc.*	3	2	1
	Цел 2: *Допълване и усъвършенстване на съществуващия нормативен режим за съществените и важни субекти в съответствие с изискванията на Директива (ЕС)2022/2555*	3	2	1
	Цел 3: *Адаптиране на съществуващата нормативна рамка в ЗКС в съответствие с изискванията на Директива (ЕС) 2022/2555, както и разширяване на компетенциите на компетентните органи по киберсигурност в Р България*	3	2	1
	Цел 4: *Регулация на присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на Националните компетентни органи*	3	2	1

5.2. По проблем 2: *Необходимостта от изграждане на координиран подход относно Директива (ЕС) 2022/2555, насочена към изграждане на способности за киберсигурност в целия Съюз, смекчаване на заплахите за сигурността на мрежите и информационните системи, използвани за предоставяне на основни услуги в ключови сектори, и осигуряване на приемственост на такива услуги при изправяне пред тях инциденти с киберсигурност, като по този начин допринася за ефективната икономика и общество на Съюза.*

		Вариант 1 „Без действие“	**Вариант 2 Максимално широк обхват и стриктна регулация“**	**Вариант 3 „Балансиран подход”**
Ефективност	**Цел 1:** *Повишаване на степента на подготвеност на съществените и важни субекти в областта на киберсигурността би довело до смекчаване на потенциалните загуби на приходи поради кибератаки и би намалило големите разходи за смекчаване на заплахите ad-hoc.*	3	2	1
	Цел 2: *Допълване и усъвършенстване на съществуващия нормативен режим за съществените и важни субекти в съответствие с изискванията на Директива (ЕС)2022/2555*	3	2	1
	Цел 3: *Адаптиране на съществуващата нормативна рамка в ЗКС в съответствие с изискванията на Директива (ЕС) 2022/2555, както и разширяване на компетенциите на компетентните органи по киберсигурност в Р България*	3	2	1
	Цел 4: *Регулация на присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на Националните компетентни органи*	3	2	1
Ефикасност	**Цел 1:** *Повишаване на степента на подготвеност на съществените и важни субекти в областта на киберсигурността би довело до смекчаване на потенциалните загуби на приходи поради кибератаки и би намалило големите разходи за смекчаване на заплахите ad-hoc.*	3	2	1
	Цел 2: *Допълване и усъвършенстване на съществуващия нормативен режим за съществените и важни субекти в съответствие с изискванията на Директива (ЕС)2022/2555*	3	2	1
	Цел 3: *Адаптиране на съществуващата нормативна рамка в ЗКС в съответствие с*	3	2	1

	изискванията на Директива (ЕС) 2022/2555, както и разширяване на компетенциите на компетентните органи по киберсигурност в Р България			
	Цел 4: *Регулация на присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на Националните компетентни органи*	3	2	1
Съгласуваност	**Цел 1:** *Повишаване на степента на подготвеност на съществените и важни субекти в областта на киберсигурността би довело до смекчаване на потенциалните загуби на приходи поради кибератаки и би намалило големите разходи за смекчаване на заплахите ad-hoc.*	3	2	1
	Цел 2: *Допълване и усъвършенстване на съществуващия нормативен режим за съществените и важни субекти в съответствие с изискванията на Директива (ЕС)2022/2555*	3	2	1
	Цел 3: *Адаптиране на съществуващата нормативна рамка в ЗКС в съответствие с изискванията на Директива (ЕС) 2022/2555, както и разширяване на компетенциите на компетентните органи по киберсигурност в Р България*	3	2	1
	Цел 4: *Регулация на присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на Националните компетентни органи*	3	2	1

** При повече от един поставен проблем мултиплицирайте таблицата за всеки отделен проблем.*

5.3. По проблем 3:*Допълване на основни сегменти, както и разширяване на икономическите сектори по Директива (ЕС) 2022/2555, осъществяване на регулацията им посредством надграждане дейността и добавяне на правомощия на националните компетентни органи*

		Вариант 1 „Без действие“	**Вариант 2 Максимално широк обхват и стриктна регулация“**	**Вариант 3 „Балансиран подход”**
Ефективно ст	**Цел 1:** *Повишаване на степента на подготвеност на съществените и важни субекти в областта на киберсигурността би довело до смекчаване на потенциалните загуби на приходи поради кибератаки и би намалило*	3	2	1

	големите разходи за смекчаване на заплахите ad-hoc.			
	Цел 2: *Допълване и усъвършенстване на съществуващия нормативен режим за съществените и важни субекти в съответствие с изискванията на Директива (ЕС)2022/2555*	3	2	1
	Цел 3: *Адаптиране на съществуващата нормативна рамка в ЗКС в съответствие с изискванията на Директива (ЕС) 2022/2555, както и разширяване на компетенциите на компетентните органи по киберсигурност в Р България*	3	2	1
	Цел 4: *Регулация на присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на Националните компетентни органи*	3	2	1
Ефикасност	**Цел 1:** *Повишаване на степента на подготвеност на съществените и важни субекти в областта на киберсигурността би довело до смекчаване на потенциалните загуби на приходи поради кибератаки и би намалило големите разходи за смекчаване на заплахите ad-hoc.*	3	2	1
	Цел 2: *Допълване и усъвършенстване на съществуващия нормативен режим за съществените и важни субекти в съответствие с изискванията на Директива (ЕС)2022/2555*	3	2	1
	Цел 3: *Адаптиране на съществуващата нормативна рамка в ЗКС в съответствие с изискванията на Директива (ЕС) 2022/2555, както и разширяване на компетенциите на компетентните органи по киберсигурност в Р България*	3	2	1
	Цел 4: *Регулация на присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на Националните компетентни органи*	3	2	1
Съгласуваност	**Цел 1:** *Повишаване на степента на подготвеност на съществените и важни субекти в областта на киберсигурността би довело до смекчаване на потенциалните загуби на приходи поради кибератаки и би намалило големите разходи за смекчаване на заплахите ad-hoc.*	3	2	1

	Цел 2: *Допълване и усъвършенстване на съществуващия нормативен режим за съществените и важни субекти в съответствие с изискванията на Директива (ЕС)2022/2555*	3	2	1
	Цел 3: *Адаптиране на съществуващата нормативна рамка в ЗКС в съответствие с изискванията на Директива (ЕС) 2022/2555, както и разширяване на компетенциите на компетентните органи по киберсигурност в Р България*	3	2	1
	Цел 4: *Регулация на присъединените сегменти, както и разширените икономическите сектори по Директива (ЕС) 2022/2555, посредством надграждане дейността и правомощията на Националните компетентни органи*	3	2	1

** При повече от един поставен проблем мултиплицирайте таблицата за всеки отделен проблем.*

6. Избор на препоръчителен вариант:

По проблем 1,2 и 3: Създаване на Проект на Закон за изменение и допълнение на Закона за Киберсигурност;

6.1. Промяна в административната тежест за физическите и юридическите лица от прилагането на препоръчителния вариант (включително по отделните проблеми):

○ Ще се увеличи

○ Ще се намали

◉ Няма ефект

……..……
……

1.1. Изборът следва да е съотносим с посочените специфични въздействия на препоръчителния вариант за решаване на всеки проблем.

1.2. Ако се предвижда въвеждането на такса, представете образуването на нейния размер съгласно Методиката по чл. 7а от Закона за ограничаване на административното регулиране и административния контрол върху стопанската дейност.

6.2. Създават ли се нови/засягат ли се съществуващи регулаторни режими и услуги от прилагането на препоръчителния вариант (включително по отделните проблеми)?

○ Да

……..……
……

◉ Не

1.1. Изборът следва да е съотносим с посочените специфични въздействия на избрания вариант.

1.2. В случай че се предвижда създаване нов регулаторен режим, посочете неговия вид (за стопанска дейност: лицензионен, регистрационен; за отделна стелка или действие: разрешителен, уведомителен; удостоверителен и по какъв начин това съответства с постигането на целите).

1.3. Мотивирайте създаването на новия регулаторен режим съгласно изискванията на чл. 3, ал. 4 от Закона за ограничаване на административното регулиране и административния контрол върху стопанската дейност.

1.4. Посочете предложените нови регулаторни режими отговарят ли на изискванията на чл. 10 – 12 от Закона за дейностите по предоставяне на услуги.

1.5. Посочете изпълнено ли е изискването на § 2 от Допълнителните разпоредби на Закона за дейностите по предоставяне на услуги.

1.6. В случай че се изменят регулаторни режими или административни услуги, посочете промяната.

6.3. Създават ли се нови регистри от прилагането на препоръчителния вариант (включително по отделните проблеми)?

○ Да

……..……
……

◉ Не

Когато отговорът е „Да“, посочете регистрите, които се създават и по какъв начин те ще бъдат интегрирани в общата регистрова инфраструктура.

6.4. По какъв начин препоръчителният вариант въздейства върху микро-, малките и средните предприятия (МСП) (включително по отделните проблеми)?

◉ Актът засяга пряко МСП

○ Актът не засяга МСП

Изборът следва да е съотносим с посочените специфични въздействия на препоръчителния вариант.

6.5. Потенциални рискове от прилагането на препоръчителния вариант (включително по отделните проблеми):

Не се идентифицират потенциални конкретни рискове, които да засягат и да бъдат свързани с прилагането на препоръчителния вариант на действие. Приемането на предложените промени със Закон за изменение и допълнение на Закона за Киберсигурност, цели да надгради и доразвие действащата към настоящия момент правна уредба и да я унифицира, по начин по-който да осигури ефективното й прилагане. Също така основната цел е да се транспонира „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“ (Директива МИС 2)

Посочете възможните рискове от прилагането на препоръчителния вариант, различни от отрицателните въздействия, напр. възникване на съдебни спорове и др.

7. Консултации:

○ Проведени са консултации

……..……
……..
……..

Посочете основните заинтересовани страни, с които са проведени консултации. Посочете резултатите от консултациите, включително на ниво ЕС: спорни въпроси, многократно поставяни въпроси и др.

◉ Предстоят обществени консултации по чл. 26 от Закона за нормативните актове

Проектът на Закон за изменение и допълнение на Закона за киберсигурност ще бъде публикуван за провеждане на обществени консултации за срок от 1 месец.

Обобщете най-важните въпроси за обществени консултации. Посочете индикативен график за тяхното провеждане и видовете консултационни процедури.

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

(•) Да

( ) Не

„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“ (Директива МИС 2) **https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32022L2555**

1.1. Посочете изискванията на правото на Европейския съюз, включително информацията по т. 6.2 и 6.3, дали е извършена оценка на въздействието на ниво Европейски съюз, и я приложете (или посочете връзка към източник).

1.2. Изборът трябва да съответства на посоченото в раздел 1, съгласно неговата т. 1.5.

9. Изисква ли се извършване на цялостна предварителна оценка на въздействието поради очаквани значителни последици?

( ) Да

(•) Не

(преценка съгласно чл. 20, ал. 3, т. 2 от Закона за нормативните актове)

10. Приложения:

Приложете необходимата допълнителна информация и документи.

11. Информационни източници:

1. „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“ (Директива МИС 2) - **https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32022L2555**
2. Закон за киберсигурност - https://lex.bg/bg/laws/ldoc/2137188253
3. Закон за административните нарушения и наказания - https://lex.bg/bg/laws/ldoc/2126821377

Посочете изчерпателен списък на информационните източници, които са послужили за оценка на въздействията на отделните варианти и при избора на вариант за действие: регистри, бази данни, аналитични материали и др.

12. Име, длъжност, дата и подпис на директора на дирекцията, отговорна за извършването на частичната предварителна оценка на въздействието:

Име и длъжност: Бисерка Радева – и.д. директор дирекция „Мрежова и информационна сигурност“

Дата: 25.06.2024г.

Подпис: … Biserka Georgieva Radeva Digitally signed by Biserka Georgieva Radeva Date: 2024.06.25 16:23:36 +03'00'