Влада на Република Северна Македонија
МИНИСТЕРСТВО ЗА ДИГИТАЛНА ТРАНСФОРМАЦИЈА

П Р И Л О Г

ИЗВЕШТАЈ ЗА ПРОЦЕНКА НА ВЛИЈАНИЕТО НА РЕГУЛАТИВАТА

Назив на министерство:	МИНИСТЕРСТВО ЗА ДИГИТАЛНА ТРАНСФОРМАЦИЈА
Назив на предлогот на закон:	ПРЕДЛОГ ЗАКОН ЗА БЕЗБЕДНОСТ НА МРЕЖНИ И ИНФОРМАЦИСКИ СИСТЕМИ (*)
Одговорно лице и контакт информации:	Тања Милановска - Најдовски 02/320-0992 tanja.milanovska@mdt.gov.mk
Вид на Извештај:	☐ Нацрт ☒ Предлог
Обврската за подготовка на предлогот на закон произлегува од:	☒ Годишна програма за работа на Владата на Република Северна Македонија ☒ НПАА ☐ Заклучок на Владата на Република Северна Македонија ☐ Друго _____
Поврзаност со Директивите на ЕВРОПСКА УНИЈА:	ДИРЕКТИВА (ЕУ) 2022/2555 НА ЕВРОПСКИОТ ПАРЛАМЕНТ И НА СОВЕТОТ од 14 декември 2022 година за мерките за високо заедничко ниво на кибербезбедност низ Унијата, за изменување на Регулативата (ЕУ) бр. 910/2014 и Директивата (ЕУ) 2018/1972 и за укинување на Директивата (ЕУ) 2016/1148 (Директива NIS 2)
Дали нацрт извештајот содржи информации согласно прописите кои се однесуваат на класифицираните информации:	☐ Да ☒ Не
Датум на објавување на нацрт Извештајот на ЕНЕР:	18.12.2024 година
Датум на доставување на нацрт Извештајот до Министерството за јавна администрација:	25.04.2025 година
Датум на добивање на мислењето од Министерството за јавна администрација:	/

Рок за доставување на предлогот на закон до Генералниот секретаријат	јуни 2025 година

1. Опис на состојбите во областа и дефинирање на проблемот

1.1 Опис на состојбите

Македонија сеуште нема закон со кој се уредува областа за безбедноста на мрежните и информациските системи и постојните мерки за сајбер безбедност се фрагментирани по сектори. Ова претставува проблем со оглед на зголемената зависност од дигитални услуги и инфраструктура во сите сектори а посебно кај енергетика, транспорт, финансии, здравство, јавна администрација и итн. Растот на сајбер нападите и сложеноста на заканите создаваат ризик од сериозни инциденти кои можат да доведат до прекини на основни услуги, финансиски загуби и да ја нарушат довербата на граѓаните во администрацијата.

Недостатокот на унифицирана законска рамка значи дека надлежностите за спречување и одговор на сајбер инциденти не се јасно дефинирани, а државните и приватните субјекти немаат стандардизирани обврски за заштита и пријавување на инциденти. Ова доведува и до други сериозни предизвици, вклучувајќи го и забавувањето на дигитализацијата, зголемените безбедносни ризици, недостатокот на правна сигурност и нарушувањето на економскиот раст и конкурентноста на земјата.

Понатаму, државата се соочува со предизвикот на сајбер закани, а овој проблем се одразува на многу области, од владините служби до здравството и финансиите, каде безбедноста на информациски системи е клучна. Сегашното законско решение е фрагментирано во посебни закони, не доволно јасно, без постоење на соодветна координација што ги прави не доволно ефикасни за да ги заштитат системите од сајбер напади. Дополнително, голем предизвик за функционирањето на државните институции е и недостатокот на човечки ресурси кои е потребно да се запознаат со основните правила на безбедноста на мрежните и инфомациските системи.

До пред донесување на Законот за изменување и дополнување на законот за организација и работа на органите на државната управа во Македонија немаше надлежна институција за сајбер безбедност. Со законот од 2024 тоа се промени и Министерството за дигитална трансформација ја презема таа надлежност.

1.2 Причини за проблемите кои се предмет на разгледување

Проблемите поврзани со безбедноста на мрежни и информациски системи во Македонија се предизвикани од неколку клучни фактори кои се истовремено глобални и локални во својата природа:

- Зголемена зависност од ИТ системи, односно државата се повеќе е зависна од информациски технологии во секој аспект и секојдневното работење. Ова ги прави системите потенцијални цели за сајбер напади, што може сериозно да влијае на националната безбедност, економијата и приватноста на личните податоци.
- Недостаток на соодветно сеопфатно законско решение, - постојните закони и политики за сајбер безбедност не се во чекор со брзите промени во технологијата и методите на напад.
- Несоодветна координација и споделување на информации, односно слаба координација помеѓу органите на државната управа, органите во состав и единиците на локалната самоуправа како и помеѓу приватниот и јавниот сектор, претставува сериозен предизвик. Исто така, недостатокот на ефективни механизми за споделување информации за заканите ја намалува можноста за рано откривање и брз одговор на сајбер инциденти.

Ресурсите и обуките, вклучувајќи инвестици во сајбер безбедноста често се ограничени, што вклучува и недостаток на обучен персонал способен да управува и одговори на сајбер закани. Тоа ја ограничува способноста на институциите да се заштитат и ефикасно да реагираат на сајбер напади.

Дополнително што во многу случаи, постојната инфраструктура и технологиите кои се користат не се во тек со современите трендови, што ги прави ранливи на напади. Модернизацијата на овие системи бара значителни финансиски средства и експертиза која често недостасува.

2. Цели на предлог регулативата

Цели на Предлог законот се изградба на капацитети за безбедност на мрежни и информациски системи во државата, намалување на заканите за мрежните и информациските системи што се користат за обезбедување основни услуги во клучните сектори и обезбедување на континуитет на таквите услуги во случај на инциденти, со што се придонесува кон безбедноста на Република Северна Македонија и ефективно функционирање на нејзината економија и општество.

Согласно одредбите од законот во иднина институциите од јавниот сектор и приватно правните субјекти опфатени со одредбите од овој закон ќе развијат соодветни човечки и технички капацитети кои ќе гарантираат безбедност на нивните мрежни и

информациски системи. Имено од 1 јануари 2026 година институциите ќе започнат со пополнување на работните места на офицери за сајбер безбедност, а ќе се започне и со набавка на соодветни технички средства за доследна примена на законот.

Дополнително институциите на јавниот сектор и приватно правните субјекти опфатени со законот од 1 јануари 2026 година ќе започнат со имплементација на соодветни мерки кои ќе ги пропишат надлежните органи, а кои ќе придонесат за намалување на заканите по безбедноста на мрежните и информациските системи. Ваквата зголемена безбедност треба да придонесе до обезбедување на континуитет на сите услуги во сите сектори што се од критично значење за државата.

3. Можни решенија (опции)

3.1 Опис на решението „не прави ништо“

Описот на решението „не прави ништо“ во контекст на проблемите со сајбер безбедноста и заканите кои се наведени претходно е сценарио каде што не се преземаат никакви нови активности или промени во постојната политика и законска рамка. Ова значи продолжување на работење според сегашните закони и мерки, без воведување на дополнителни заштити или адаптации кои би одговориле на сè пораснатите и пософистицирани сајбер закани. За државата тоа би значело дека постоечките закони стануваат нерелевантни и неефикасни. Без ажурирања и адаптации, системот за сајбер безбедност останува подложен на инциденти. Исто така недостигот јасна структура на надлежности може сериозно да ја наруши националната безбедност, да предизвика значителни финансиски загуби и да има штетни последици врз довербата на граѓаните и приватните правни лица.

Останувањето на статус-куо и избегнувањето на воведување нови мерки и политики би значело пропиштена можност да се изградат подобри капацитети и ресурси за превенција и реагирање на сајбер закани.

Решението „не прави ништо“ е ризично и потенцијално штетно затоа што не ја адресира растечката потреба за зајакнување на сајбер безбедноста во современиот дигитален свет. Оваа опција би можела да резултира со продолжување на постојните проблеми и недостатоци, што би можело дополнително да го комплицира идно управување со сајбер заканите.

3.2 Опис на можните решенија (опции) за решавање на проблемот

Во моментов сајбер безбедноста не е системски уредена со закон. Во определени области, како што е енергетиката или електронските комуникации има определена

законска регулација, меѓутоа сето тоа не е доволно за системско решавање на проблемот со безбедноста на мрежните и информациските системи кој станува се позначаен со развојот на дигиталното општество. Поради тоа е неопходно со едно системско законско решение да се уреди сајбер безбедноста. Со законот чие донесување се предлага се уредуваат институциите од јавниот сектор и секторите на кои припаѓаат субјектите на кои се однесува законот, се утврдуваат надлежните органи за управување со сајбер кризи, значајни сајбер безбедносни инциденти и сајбер безбедносни инциденти со голем опфат, единствената точка за контакт за сајбер безбедност и тимовите за одговор на инциденти со компјутерска безбедност, се уредуваат мерките за безбедност на мрежни и информациски системи и за управување со ризикот за сајбер безбедност, обврските за известување за сите аспекти на безбедност на мрежни и информациски системи за правните лица кои обезбедуваат услуги во критични сектори, правилата и обврските за известување и размена на информации за инциденти, обврската за усвојување на стратешкиот документ кој ја опфаќа безбедноста на мрежните и информациските системи, надзорот над спроведувањето на одредбите од законот, како и други прашања поврзани со безбедност на мрежни и информациски системи. Со уредување на сите овие прашања ќе се овозможи ефикасен механизам за сајбер безбедност, почнувајќи од воспоставување на соодветна институционална рамка, преку утврдување на конкретни мерки и активности кои ќе треба да се преземат, се до воспоставување на механизам за надзор над спроведување на законот и соодветни санкции. Сето тоа како целина ќе овозможи државата да ги прифати најсовремените трендови во делот на безбедноста на мрежните и информациските системи.

4. Проценка на влијанијата на регулативата

Можни позитивни и негативни влијанија од секоја од опциите:

4.1 Економски влијанија

Можните економски влијанија од предложениот Закон за безбедност на мрежни и информациски системи се значајни за развој на областа во државата. Првенствено, воведувањето на мерки за сајбер безбедност би можело да доведе до значителни почетни инвестиции од страна на државата и приватниот сектор за ажурирање на технолошката инфраструктура и системите за безбедност. Ова вклучува купување на напредно безбедносно опрема, софтвер и услуги, што би можело значително да ја зголеми потрошувачката во ИТ секторот, стимулирајќи економски раст и развој.

Дополнително, подобрената сајбер безбедност би можела да создаде поголема доверба кај потрошувачите и бизнисите, што е клучно за дигиталната економија. Ова би можело да предизвика зголемување на електронската трговија, дигиталните трансакции и онлајн услугите, со што се засилува економскиот раст. Исто така, јакнењето на сајбер безбедносните капацитети може да привлече странски инвестиции, особено во сектори кои се особено чувствителни на сајбер ризици како што се финансиите и здравството.

На долг рок, ефикасната имплементација на законот може да помогне во намалувањето на трошоците поврзани со сајбер инциденти, како што се измамите, кражбите на податоци и прекините во работењето. Овие заштеди можат значително да ги намалат економските загуби и да овозможат понатамошни реинвестирања во иновации и безбедносни технологии. Со добро управување и спроведување, законот има потенцијал значително да придонесе кон стабилноста и отпорноста на националната економија против сè почести и пософистицирани сајбер закани.

Негативни економски влијанија

Сепак, воведувањето на овие законски промени носи и одредени ризици и потенцијални негативни влијанија. Најзначајни се почетните високи трошоци за компаниите кои можеби ќе се соочат со финансиски тешкотии при нивното исполнување. Покрај тоа, зголемената регулатива може да донесе дополнителни оперативни товари и да ограничи агилноста и иновативноста на бизнисите, што потенцијално може да ја забави имплементацијата на нови технологии и да намали конкурентноста на домашните компании на глобалниот пазар.

Во случајот на **„неправи ништо“**, нема да има дополнителни економски влијанија.

4.2 Фискални влијанија

Фискалните влијанија на предложениот закон, а во насока на унапредување на сајбер безбедноста се значајни, особено во однос на потребите за финансиски ресурси за поддршка на оперативни аспекти. Првично, зголемениот фискални трошоци ќе произлегуваат од неопходноста за набавка на софистицирана опрема за основање и функционирање на владиниот тим за одговор на компјутерски инциденти (ЦИРТ). Ова вклучува набавка на хардвер и софтвер кои се клучни за заштита на мрежите и системите од напади, како и трошоци за одржување и ажурирање на истите. За ова цел ќе бидат потребни 225.500.000,00 денари годишно, во следните три години (2026, 2027 и 2028), односно вкупно, 676.500.000,00 денари. Овие проценки се направени врз основа на утврдување на опремата и софтверите кои ќе треба да се набават во следниот период, а

кои се неопходни за доследно спроведување на законот. При тоа се користени и компаративни искуства од други држави.

Покрај капиталните инвестиции во опрема, друг значителен фискален товар е со платите за вработените во организациската единица за сајбер безбедност во Министерството за дигитална трансформација, вработените во секторските надлежни органи, вработените во тимовите за одговор на компјутерски инциденти и офицерите за сајбер безбедност во државните институции. Овие трошоци вклучуваат додаток на плата во износ од 40% од постојната плата на вработените. Имајќи го во предвид опфатот на субјектите, овој додаток е предвиден за 80 административни службеници со звање советник, и вкупно изнесува 27.264.000,00 денари. При тоа за правата година, додатокот за плата е предвиден само за последните 4 месеци, а фискалните импликации за истиот изнесуваат 6.816.000,00 денари

Вкупните фискални импликации на годишно ниво во периодот 2026-2028 година изнесуваат 252.764.000,00 денари. Од 2029 година фискалните импликации се 27.264.000,00 денари годишно.

Во случајот на **„неправи ништо“**, нема да предизвика дополнителни финансиски влијанија.

4.3 Социјални влијанија

Позитивни влијанија: Зголемувањето на сајбер безбедноста преку новиот предлог закон ќе ја подобри заштитата на личните податоци и ќе ја зголеми довербата на граѓаните во држвните ИКТ системи. Подобрата безбедност може да поттикне поголема употреба на онлајн услуги и да ја заштити приватноста на луѓето.

Негативни влијанија: Строгите мерки за безбедност може да создадат загриженост кај граѓаните за нивните лични слободи, особено ако се доживее како ограничување на приватноста. Плус, новото законско решение може да предизвика дигитален јаз меѓу оние со пристап до новите технологии и оние без таков пристап, што може да влијае на социјалната еднаквост.

Во случајот на **„неправи ништо“** би довело до дискриминација на лицата со попреченост, како и неможноста за обезбедување на инклузивно општество.

4.4 Влијанија врз животната средина

Позитивни влијанија: Еден од потенцијалните позитивни влијанија на Предлог законот за сајбер безбедност е намалувањето на физичкиот отпад. Со промовирање на дигитализација и онлајн услуги, може да се намали употребата на хартиени документи,

што директно придонесува кон намалување на потребата за сеча на дрвја и производство на хартија, намалување на отпадот и емисиите од транспорт на физички документи.

Негативни влијанија: Сепак, зголемената употреба на ИТ технологија и податочни центри за поддршка на зголемените потреби за сајбер безбедност може да имаат негативни влијанија врз животната средина. Оваа инфраструктура бара значителна зголемена потрошувачка на електрична енергија, што може да придонесе и кон зголемено загадување, особено ако енергијата доаѓа од необновливи извори. Исто така, одржувањето на овие системи може да предизвика генерирање на електронски отпад, кој често содржи штетни материјали што може негативно да влијаат на околината ако не се рециклираат правилно.

Во случајот на **„неправи ништо“**, може да ја зголеми потребата од сечење на дрвја, а со тоа и да се зголеми отпадот од хартија, што би имало негативно влијание врз животната средина.

4.5 Административни влијанија и трошоци –

а) трошоци за спроведување

Заради спроведување на специјализирани обуки за вработените, субјектите на министерството ќе треба да плаќаат соодветен надомест на Министерството за дигитална трансформација, кој ќе биде око 6100,00 денари по ден обука.

Дополнително субјектите кои ќе сакаат да се сертифицираат за независни ревизори ќе треба да плаќаат административна такса во износ од 250,00 денари.

На крај заради спроведување на надворешни ревизии, субјектите ќе треба да плаќаат соодветен надомест, согласно пазарните цени за ревизијата.

Во случајот на **„неправи ништо“**, примената на досегашното решение нема да предизвика дополнителни трошоци за спроведување на регулативата.

б) трошоци за почитување на регулативата

Трошоците за имплементација на ова законско решение ќе вклучуваат почетни инвестиции за опрема (хардвер и софтвер), безбедност, обука, правни консултации и техничка поддршка, како и континуирани трошоци за одржување на системот. Сепак, долгорочно, овие трошоци можат да се надоместат преку повеќе безбедни државни ИКТ системи, безбедни јавни услуги, повеќе заштеди и повеќе економска активност, како и зголемени приходи од даноци и намалени трошоци.

5. Консултации

5.1 Засегнати страни и начин на вклучување

///

5.2 Преглед на добиените и вградените мислења

Во прилог на овој ПВР Извештај е табела со пристигнати мислења кои се вградени во предлог законот.

5.3 Мислењата кои не биле земени предвид и зошто

Во прилог на овој ПВР Извештај е табела со пристигнати мислења кои не се земени во предвид и образложение за истото.

6. Заклучоци и препорачано решение

6.1 Споредбен преглед на позитивните и негативните влијанија на можните решенија (опции)

Доколку се прифати решението „не прави ништо“ безбедноста на мрежните и информациските системи повторно ќе остане сива област, која не е целосно уредена, поради што ризиците по безбедноста ќе биде огромна, што во случај на инцидент може да го наруши редовното функционирање на државата и на економските текови.

Со донесувањето на ова законско решение ќе има значителни позитивни влијанија како што се повеќе ефикасни јавни услуги, поголема транспарентност, и поддршка на економскиот раст. Меѓутоа, исто така постојат негативни влијанија кои вклучуваат високи почетни трошоци, ризици за приватноста и можни технолошки бариери за одредени социјални групи. Клучен е балансот помеѓу овие влијанија за да се обезбеди успешна имплементација на системот.

6.2 Ризици во спроведувањето и примената на секое од можните решенија (опции)

Со донесувањето на новото законско решение постојат неколку потенцијални ризици во спроведувањето и примената: недоволни финансиски ресурси, недостаток на техничка експертиза, отпор кон промени, недоволен мониторинг, технолошки застарени системи, неприфатеност од корисниците. Постои можност корисниците да не бидат доволно информирани или да не ги разберат придобивките од овие промени, што може да доведе до ниска употреба на новите или прилагодените решенија.

Доколку остане моменталното решение, таа значи дека државата не ги почитува обврските за усогласување на националното законодавството со правото на Европска Унија, што претставува закана и пречка за напредокот на државата кон членство во Европската Унијата.

Дополнително, ако остане моменталното решение тоа би значело дека Република Северна Македонија може да се соочи со сериозни предизвици, вклучувајќи забавување на дигитализацијата, поголеми безбедносни ризици, недостаток на правна сигурност и невозможност за економски раст и конкурентност. Понатамошно одложување на имплементацијата може да ја ограничат земјата во нејзината способност да се интегрира во глобалната дигитална економија.

6.3 Препорачано решение со образложение

Со Законот за безбедност на мрежна и информациска безбедност се исполнува една од обврските од Реформаската Агенда на Западен Балкана што се однесува на Македонија. Законот обезбедува високо ниво на безбедност на личните податоци, преку примена на напредни технологии како криптографија и двофакторска автентикација. Ќе се создаде правна рамка која ќе гарантира заштита на правата на корисниците и ќе ги стандардизира дигиталните услуги според европските и глобалните практики. Ова решение ќе овозможи интеграција на Република Северна Македонија во европскиот дигитален пазар, што ќе поттикне економски раст и привлекување странски инвестиции. Во исто време, ќе се поддржи инклузивноста на сите граѓани, осигурувајќи безбеден пристап до сите државни системи без разлика на нивниот социјален статус или локација.

7. Спроведување на препорачаното решение

7.1 Потреба од менување на закони и подзаконска регулатива во областа или други сродни области

По донесување на законот, со истиот ќе треба да се усогласат Законот за електронски комуникации и Законот за електронски документи, електронска идентификација и доверливи услуги.

7.2 Потребни подзаконски акти и рок за нивно донесување

1. Уредба за начинот на идентификација на секторите, потсекторите и видовите субјекти заради утврдување на детална листа на потсектори и видови на субјекти од секторите со висока критичност, детална листа на потсектори и видови на субјекти во другите критични сектори од член, детална листа на суштински субјекти, детална листа на важни субјекти, формата и содржината на деталните листи, како и формата, содржината и начинот на водење на регистрите на сектори со висока критичност, на други критични сектори, на суштински субјекти и на важни субејкти – член 7 став (10)

2. Методологијата за проценка на ризик заради утврдување на суштинските субјекти, како и методологијата за проценка на ризик заради утврдување на важните субјекти – член 8 став (3).
3. Правилник за поблиските критериуми во однос на големината и обемот на работа за формирање на организациска единица, односно областување на офицер за сајбер безбедност ги пропишува министерот член 8 став (7).
4. Правилник за начинот на работа на Тимот за одговор на компјутерски инциденти во случаите кога инцидентите со голем опфат не довеле до прогласување на кризна состојба – член 19 став (6).
5. Правилник за начинот на пријава и постапување по пријавени или идентификувани инциденти на мрежните и информатичките системи – член 22 став (2).
6. Методологијата за спроведување на анализата на ризик за приоретизирање на одредени задачи – член 24 став (6)
7. Правилник за потребните стручни квалификации, општи и посебни комепетенции за офицер за сајбер безбеднос – член 25 став (11);
8. Правилник за техничките и методолошките барања за мерките на суштинските субјекти и важните субјекти кои се однесуваат на давателите на ДНС услуги, Единствениот регистар на имиња на врвни домени, даватели на услуги за компјутерска обработка во облак, даватели на услуги за податочен центар, даватели на услуги за мрежи за испорака на содржини, даватели на управувани услуги, даватели на управувани безбедносни услуги, даватели на услуги на интернет продажба, даватели на услуги на интернет-пребарувач и даватели на платформи за услуги за социјални мрежи, како и даватели на доверливи услуги – член 32 став (5)
9. Правилник за начинот на размена на податоците во рамките на суштинските субјекти и важните субјекти и каде што е релевантно и со нивните добавувачи или даватели на услуги, како и процедурите за размена на информации – член 38 став (6);
10. Програма за специјализирана обука за офицер за сајбер безбедност, програмата за генеричките обуки, начинот на нивна реализација, висината на надоместокот, формата содржината и сертификатот за поминатата обука – член 39 став (9);
11. Правилник за Формата и содржината на службената легитимација за овластеното лице за стручен надзор и начинот на нејзиното издавање - член 42 став (4);
12. Правилник за потребните стручни квалификации, општи и посебни комепетенции на овластеното лице за стручен надзор - член 42 став (5);

13. Правилник за образецот на формата и задолжителните елементи на записникот од извршениот надзор – член 46 став (6);
14. Упатства и процедури што се спроведуваат при оценување на информацискатa безбедност на мрежните и информациските системи на Владата, министерствата, самостојните органи на државната управа, органите на државната управа во состав на министерствата, управните организации, општините, општините во Градот Скопје и Градот Скопје – член 12 став (1) точка 6);
15. Упатства и пропишува процедури што се спроведуваат при оценување на информацискатa безбедност на мрежните и информациските системи на субјектите за кои е надлежен– член 16 став (1) точка 2);

Ѓ Подзаконските акти ќе се донесат во рок од една година од денот на стапување на сила на овој Предлог закон.

7.3 Органи на државната управа, државни органи и други органи надлежни за спроведување

Надлежен орган ќе бидат Министерството за дигитална трансформација.

7.4 Активности за обезбедување на ефикасно спроведување на предлогот на закон

Заради ефикасно спроведување на законот, покрај уредувањето на стандардите за безбедност на мрежните и информациските системи ќе се преземат и активности за промоција на новите законски обврски и подигање на свеста кај граѓаните за сајбер хигиената преку информативни кампањи. Дополнително ќе се спроведат специјализирани обуки за лицата кои ќе бидат одговорни за сајбер безбедноста, како и нивна сертификација. Сите вработени во јавниот сектор ќе поминат и генерички обуки за основните аспекти на сајбер безбедноста.

8. Следење и евалуација

8.1 Начин на следење на спроведувањето

Следење на примената на законот врши Министерството за дигитална трансформација и другите надлежни органи. Имено надлежните органи ќе бидат одговорни за спроведување стручен надзор над спроведување на законските обврски од страна на субјектите кои се опфатени со законот, со што ќе се следи примената на законот. Дополнително ќе биде воспоставен и Национален регистар на сајбер инциденти во кој ќе бидат содржани сите значајни сајбер инциденти кои се случиле во тековната година, а за

кои еднаш годишно Министерството за дигитална трансформација ќе ја информира Владата. На крај со законот е предвиден и стратешки документ за сајбер безбедност чија имплементација исто така ќе биде следена од министерството.

8.2 Евалуација на ефектите од предлогот на закон и рокови

Евалуацијата на ефектите од предлог на законот и рокови, врз основа на следните индикатори:

- На крајот од секоја година ќе се следи број на институции кои назначиле офицери за сајбер безбедност;
- На крајот од секоја година ќе се подготвува извештај за бројот на институции кои ги воспоставиле и ги почитуваат стандардите за сајбер безбедност;
- На годишно ниво до Владата ќе се доставува Годишен извештај за број на пријавени сајбер закани, број на пријавени напади и број на спречени напади.

Изјава од државниот секретар

Нацрт Извештајот за проценка на влијанието на регулативата е изготвен во согласност со Методологијата за проценка на влијанието на регулативата. Тој дава реална проценка на можните влијанија и очекуваните ефекти, како и трошоците кои се однесуваат на секоја од утврдените можни решенија (опции) за решавање на проблемот.

Датум:_____

_____

потпис на државен секретар

Изјава од министерот

Врз основа на резултатите од анализите прикажани во Извештајот за проценка на влијанието на регулативата сметам дека препорачаното решение (опција) претставува најдобар начин за решавање на проблемот и постигнување на очекуваните ефекти на најекономичен начин.

Датум:_____

_____

потпис на министерот