АНАЛИЗА ЕФЕКАТА ЗАКОНА О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

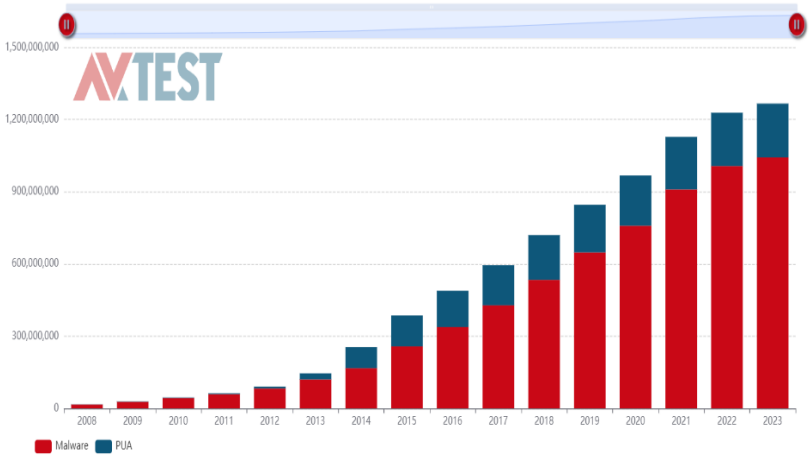
1) Који показатељи се прате у области, који су разлози због којих се ови показатељи прате и које су њихове вредности?

У области информационе безбедности показатељи који се прате односе се на:

- примену мера заштите од безбедносних ризика у информационо-комуникационим системима и
- инциденте који значајно угрожавају информациону безбедност, а којима су изложени ИКТ системи од посебног значаја.

У Стратегији за дигиталну декаду ЕУ наведено је да је процена глобалне штете од инцидената - сајбер напада у 2020. години била око 5.5 трилиона евра. Процењује се да је око 12% компанија у ЕУ било на неки начин погођено сајбер нападом, док је само 2019. године забележено 450 инцидената који су погодили критичну инфраструктуру ЕУ. Евидентан проблем је и недостатак радне снаге са проценом да око 291.000 понуда за посао у области информационе безбедности нису реализоване.

Број малвера и потенцијално нежељених апликација је у сталном порасту. Према подацима независног института AV-TEST GmbH из Магдебурга, сваког дана појави се преко 450.000 нових узорака.



Дијаграм 1 Број малициозних софтвера

Како би се ефикасније борила против изазова којих је свакодневно све више у сајбер простору, Европска унија је, по питању информационе безбедности, одредила пет стратешких приоритета:

- Постизање еластичности – системи се аутоматски опорављају након инцидента;
- Драстично смањење сајбер криминала;
- Развој политике сајбер одбране и капацитета сагласних Заједничкој безбедносној и одбрамбеној политици (CSDP);
- Развој индустријских и технолошких ресурса за информациону безбедност;
- Успостављање повезаних међународних политика информационе безбедности за ЕУ.

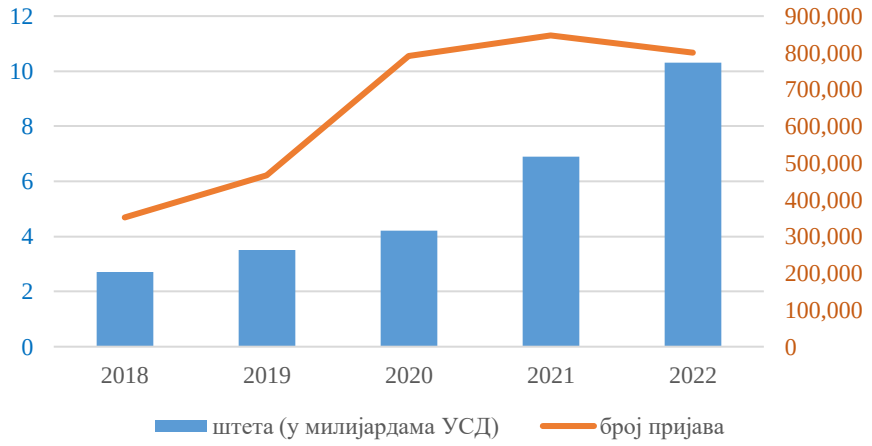
Наведени приоритети у претходним деценијама реализовали су се кроз следеће активности:

- 1992. године донета је Одлука Савета у вези безбедности информационих система
- 2004. године оснива се Европска агенција за мрежну и информациону безбедност (ЕНИСА)

- прва Стратегија безбедности информационог друштва доноси се 2006. године
- 2008. године доноси се Директива Савета за идентификацију и одређивање европске критичне инфраструктуре и процена потребе за побољшањем заштите
- 2009. године усваја се Акциони план за заштиту критичне информационе инфраструктуре
- 2012. године Европска унија формира ЦЕРТ_ЕУ
- 2013. године усваја се Стратегија информационе безбедности ЕУ
- 2016. године доноси се Директива о мерама за висок заједнички ниво безбедности мрежа и информационих система широм Уније (НИС Директива)
- 2019. године доноси се Акт о сајбер безбедности ЕУ којим су дата нова овлашћења агенцији ЕНИСА.

Сајбер криминал је свакако најзаступљенији облик злонамерног деловања у сајбер простору, уз друге облике у које спадају сајбер шпијунажа, сајбер тероризам, хактивизам и сајбер ратовање. У свом последњем извештају[1] Европски центар за сајбер криминал (енг. *European Cybercrime Centre*) наводи да је у околностима пандемије сајбер криминал еволуирао и да је то тренд који ће се наставити. Примери прилагођавања су: злоупотребе небезбедних РДП протокола (енг. *Remote Desktop Protocol*) и рањивих ВПН конекција (енг. *virtual private network*), злоупотребе повећане онлајн куповине и коришћење мобилног банкарства за имплементацију малвера или крађу креденцијала и личних података, али и све већа и напреднија употреба метода социјалног инжењеринга.

Центар за жалбе на интернет криминал америчког Федералног истражног бироа је у 2022. години примио 800.944 пријава са штетом процењеном на преко 10 милијарди долара.[2] Забрињавајући податак је да је број пријава у односу на претходну годину мањи за око 5%, али је укупна штета већа за око 49%, што указује да криминалци усавршавају своје вештине.



Дијаграм 2 Пријаве и штете на годишњем нивоу

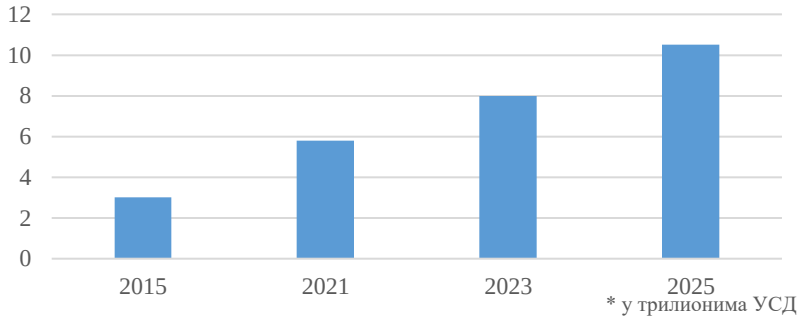
Компанија *Cybersecurity Ventures*, која израђује годишње извештаје о стању сајбер криминала[3], процењује да ће у 2024. години штете од сајбер криминала достићи осам трилиона америчких долара, што превазилази процењене приходе од трговине свих наркотика заједно. Према

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

[2] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[3] https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

доступним подацима, штете од сајбер криминала расту по стопи од 15% годишње и процењује се да ће у 2025. години прећи суму од 10 трилиона долара.

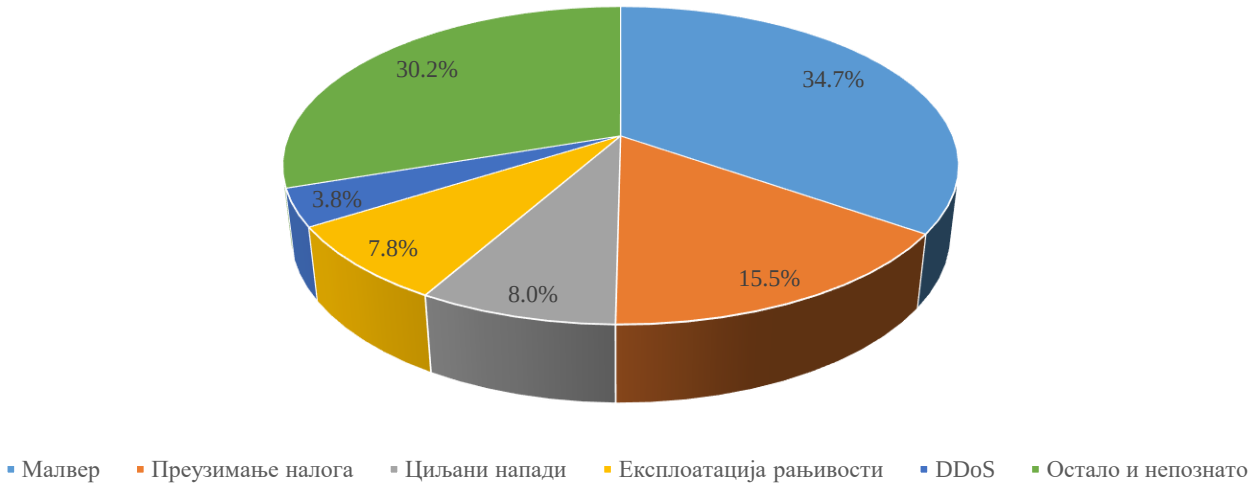


Дијаграм 3 Укупна штета од сајбер криминала

Иста компанија у свом извештају износи податке о недостатку радне снаге, са проценама да је у овом тренутку на светском нивоу непопуњено 3,5 милиона радних места у области информационе безбедности, од чега 700.000 само у САД. Илустративан је податак да је у тренутку писања тог извештаја у САД било 106.000 отворених понуда за посао за стручњаке са CISSP сертификатом (енг. *Certified Information Systems Security Professional*), док је укупан број таквих сертификата издатих у САД нешто преко 90.000. Такође је идентификован и проблем задржавања радне снаге, а посебно најквалитетније и најобученије, са податком да 24% главних службеника за информациону безбедност (CISO) у 500 највећих компанија промени посао након годину дана.

Како би се одговорило на претње у сајбер простору које се из дана у дан повећавају, неопходно је континуирано унапређивати стратешки, институционални и правни оквир у области информационе безбедности која, пре све, треба да обезбеди превентивно деловање на ове претње.

Према подацима са сајта *hackmageddon.com*, на глобалном нивоу 2022. године најзаступљенији тип напада био је коришћење малвера, док су мање заступљени (али са значајним процентом) били преузимање налога, циљани напади, искоришћавање рањивости и дистрибуирано ометање сервиса (DDoS).



Дијаграм 4 Заступљеност различитих типова инцидената у свету

Агенција ЕУ за сајбер безбедност - ЕНИСА (енг. *The European Union Agency for Cybersecurity*) објавила је у марту 2023. године студију ***Утврђивање претњи и изазова информационе безбедности за 2030. годину***, која садржи предвиђања будућих претњи и могуће противмере. Примарни циљ студије је да идентификује и прикупи информације о будућим претњама које би могле да утичу на инфраструктуру и услуге Европске уније, као и на безбедност грађана и друштва у целини. У израду студије укључени су футуристи, социолози, пословни лидери, стручњаци за информациону безбедност и други, а циљна група су национални органи за информациону безбедност, доносиоци одлука у Европској унији и земљама чланицама, тимови за реаговање, стручњаци у овој области и све друге заинтересоване стране.

Студија је идентификовала 21 претњу, од којих је издвојено десет најзначајнијих:

- компромитација ланца снабдевања,
- напредне кампање дезинформисања,
- повећање дигиталног надзора/губитак приватности,
- људске грешке и експлоатација наслеђених система,
- циљани напади побољшани злоупотребом података са паметних уређаја,
- недостатак анализе и контроле инфраструктуре и објеката у свемиру,
- напредне хибридне претње,
- недостатак обучене радне снаге,
- прекогранични пружаоци ИКТ услуга као јединствена тачка прекида (енг. *single point of failure*),
- злоупотреба вештачке интелигенције.

Пратећи стање у овој области Република Србија је усвојила Закон о информационој безбедности 28. јануара 2016. године, који је делимично пренео Директиву 2016/1148 о мерама за висок заједнички ниво безбедности мрежних и информационих система у Европској унији[4] (енг. *Network and Information Security Directive - NIS Directive*, у даљем тексту: НИС директива), с обзиром да је усвојен пре доношења те директиве.

Закон појам информационе безбедности дефинише као скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица. Предметни закон представља оквир за уређење безбедности информационо-комуникационих система у Републици Србији. Овим законом се уређују мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите.

Сходно томе, оператори ИКТ система од посебног значаја дужни су да донесу акт о безбедности ИКТ система и дефинишу мере заштите, а нарочито принципе, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја.

Поред тога, овим законом се у оквиру Регулаторног тела за електронске комуникације и поштанске услуге (у даљем тексту РАТЕЛ) успоставља Национални центар за превенцију и

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, доступна на адреси: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016L1148

заштиту од безбедносних ризика у ИКТ системима у Републици Србији (у даљем тексту: Национални ЦЕРТ), који прати стање о инцидентима о националном нивоу, обавештава релевантна лица о ризицима и инцидентима, реагује по пријављеним инцидентима, израђује анализе ризика и инцидената и подиже свест друштва о значају информационе безбедности. Једна од важних функција Националног ЦЕРТ-а је и сарадња са истим институцијама из других земаља. Имајући у виду да инциденти у ИКТ системима најчешће имају прекогранични карактер, односно да се дешавају на територији више земаља, међусобна сарадња ЦЕРТ-ова је од изузетног значаја, како би се међусобном разменом информација успешно одговорило на инциденте. Од 1. новембра 2017. године Национални ЦЕРТ је уврштен у списак међународне организације за сарадњу и размену информација из области информационе безбедности *Trusted Introducer*, а налази се и на листи ЦЕРТ тимова Агенције ЕУ за сајбер безбедност - ЕНИСА.

У оквиру Канцеларије за информационе технологије и електронску управу формиран је Сектор за информациону безбедност који, у складу са Законом, спроводи активности ЦЕРТ-а републичких органа.

У циљу спровођења Закона и у Министарству унутрашњих послова формиран је Центар за реаговање на нападе на информациони систем МУП-а (ЦЕРТ МУП) који се од јула 2016. године налази на листи ЦЕРТ тимова Агенције ЕУ за сајбер безбедност - ЕНИСА, а у новембру 2018. године добио је и акредитацију од стране сервиса *Trusted Introducer*.

Иако се са применом Закона започело одмах по усвајању, утврђено је да је неопходно извршити додатне измене и допуне законске регулативе ради усклађивања са НИС директивом која је у међувремену усвојена, али и ради унапређења неких од постојећих решења у циљу ефикаснијег спровођења закона у пракси. Због тога су у октобру 2019. године усвојене измене и допуне Закона о информационој безбедности[5] који је у потпуности усклађен са наведеном Директивом.

Изменама и допунама Закона о информационој безбедности, који је усвојен у октобру 2019. године уређене су новине које се тичу:

- надлежности и потребних капацитета Националног ЦЕРТ-а;
- укључивања Народне банке Србије у рад Тела за координацију послова информационе безбедности;
- успостављања Евиденције оператора ИКТ система од посебног значаја;
- успостављања обавезе достављања статистичких података о инцидентима који се десе у ИКТ системима од посебног значаја на годишњем нивоу;
- сарадње ЦЕРТ-ова у Републици Србији;
- заштите деце при коришћењу информационо-комуникационих технологија;
- класификовања инцидената и поступања надлежних органа у зависности од нивоа опасности инцидента.

Инспекцијским надзором над радом оператора ИКТ система од посебног значаја утврђује се да ли су оператори донели акт о безбедности и применили мере заштите, односно да ли је успостављен адекватан ниво безбедности система. Инспекцијски надзор спроводи се од 2019. године и показује, поред поштовања законских одредби, недостатак капацитета за адекватно реаговање на инциденте.

Оператори ИКТ система од посебног значаја у складу са Законом обавезни су да обавесте Надлежни орган, односно Министарство информисања и телекомуникација (у даљем тексту

[5] "Службени гласник РС", бр. 6 од 28. јануара 2016, 94 од 19. октобра 2017, 77 од 31. октобра 2019., доступан на адреси: http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2016/6/5/reg

Министарство) о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности.

У циљу бољег разумевања постојећег стања у области информационе безбедности, значајно је сагледати инциденте који су пријављени Националном ЦЕРТ-у у претходних неколико година. Ова статистика може бити значајан показатељ да ли су постојеће превентивне мере довољне и у ком правцу је потребно унапређивати правни и институционални оквир. Закон о информационој безбедности, обавезује операторе ИКТ система од посебног значаја да достављају обавештења о инцидентима који значајно нарушавају информациону безбедност ИКТ система. На основу добијених обавештења о инцидентима Национални ЦЕРТ израђује годишње статистичке извештаје који су јавно доступни путем веб презентације.

Инциденти су сврстани у 10 група:

- инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енг. malware),
- неовлашћено прикупљање података,
- превара,
- покушај упада у ИКТ систем,
- упад у ИКТ систем,
- недоступност или ограничена доступност ИКТ система,
- угрожавање безбедности података,
- оперативни инциденти,
- инциденти физичко-техничке безбедности и
- остали инциденти.

У 2022. години статистички најзаступљенији били су инциденти из групе Неовлашћено прикупљање података са преко седам и по милиона пријављених случајева, док су следећи по бројности инциденти из групе Покушаји упада у ИКТ систем са готово три милиона пријава. Број пријава у осталим групама је знатно мањи па тако у групи Преваре има преко 58 хиљада, у групи Инсталирање злонамерног софтвера у оквиру ИКТ система близу 55 хиљада, а у групи Оперативни инциденти преко 13 хиљада пријава. Укупан број пријава у осталих пет група је око шест хиљада.

Дијаграм 5 Број пријављених инцидената у Србији по групама у 2022. години

Посматрано појединачно према врсти инцидента, у 2022. години највише пријава односило се на скенирање портова које је уочено у преко 7 милиона случајева и које не наноси директну штету жртви, али представља индикативне активности нападача у фази извиђања. Пракса нападача је да овакве нападе покрећу према великом броју ИП адреса у покушају да нађу потенцијалне жртве

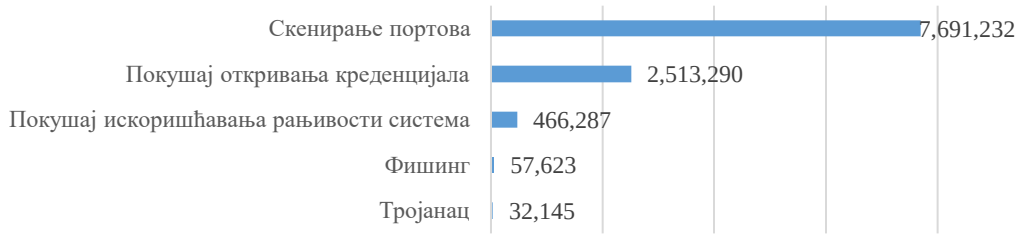
које имају незаштићене портове, па се на тај начин и ИП адресе оператора критичне инфраструктуре нађу у том опсегу.

На другом месту по бројности налази се покушај откривања креденцијала који подразумева покушај приступа систему жртве узастопним испробавањем великог броја различитих комбинација слова, бројева и симбола са циљем идентификације корисничког имена и лозинке. Ова врста напада ослања се на недостатак свести корисника приликом креирања лозинки за приступ систему и веома је популарна међу нападачима јер злоупотребом легитимног налога може бити омогућен приступ читавом ИКТ систему.

Покушај искоришћавања рањивости система је на трећем месту, а ова врста напада могућа је уколико у систему постоје рањивости.

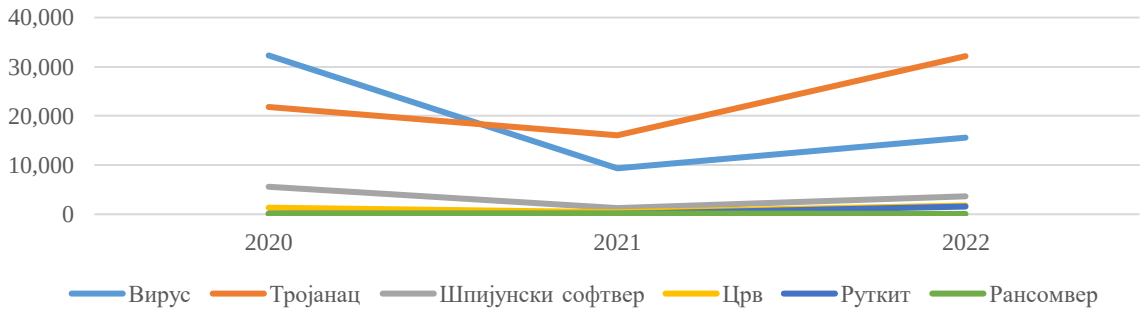
На четвртом месту по бројности налазе се фишинг напади, који су током 2022. године често били усмерени на кориснике поштанских услуга и платформи за е-трговину преко неколико великих фишинг кампања.

На петом месту су тројанци, који по покретању могу да преузму друге претње са Интернета, убацују друге типове малвера на угрожене рачунаре, комуницирају са удаљеним нападачима, бележе све што се куца на тастатури и шаљу нападачима, као и да на друге начине буду део комплекснијих сајбер напада.



Дијаграм 6 Најчешће пријављени инциденти у Србији у 2022. години

Прегледом броја инцидената по врстама за једну годину може се стећи слика о тренутном стању, али за дубљу анализу потребно је посматрати трендове у неком временском периоду. Трендови за сваку групу инцидената представљени су на наредним дијаграмима.

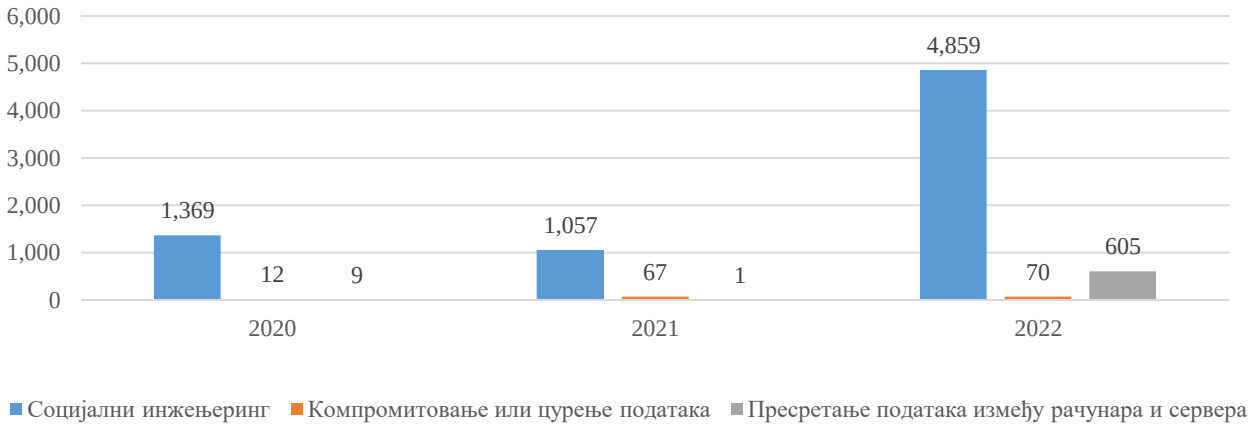


Дијаграм 7 Инциденти у групи Инсталирање злонамерног софтвера у оквиру ИКТ система

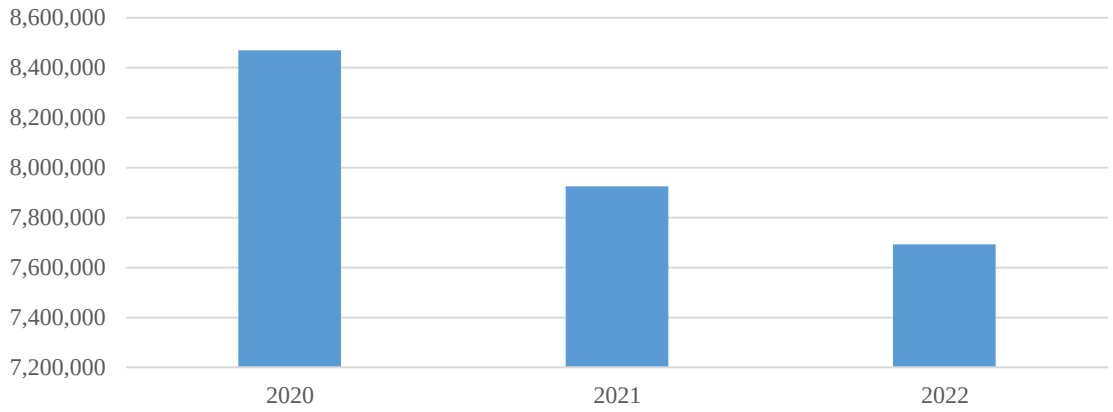
У групи Инсталирање злонамерног софтвера у оквиру ИКТ система прате се подаци за шест врста злонамерног софтвера (малвера): вирусе, тројанце, црве, руткит, рансомвер и шпијунски софтвер. Након драстичног пада броја пријава случајева инцидената код којих је коришћен злонамерни софтвер у 2021. години у односу на претходну годину, 2022. године је дошло до значајног пораста

броја инцидента који спадају у ову групу, а укупан број инцидената у овој групи готово се изједначио са бројем забележеним 2020. године.

Тројанци су најчешћи тип малвера који је коришћен у последње две године са уделом од преко 50% од свих злонамерних софтвера. Карактеристика тројанаца је да покушавају да наведу кориснике да их покрену тако што се претварају да су корисни програми, па за њихову успешну дистрибуцију нападачи укључују и методе социјалног инжењеринга.



Дијаграм 8 Инциденти у групи Неовлашћено прикупљање података (осим скенирања портова)



Дијаграм 9 Инциденти типа Скенирање портова из групе Неовлашћено прикупљање података

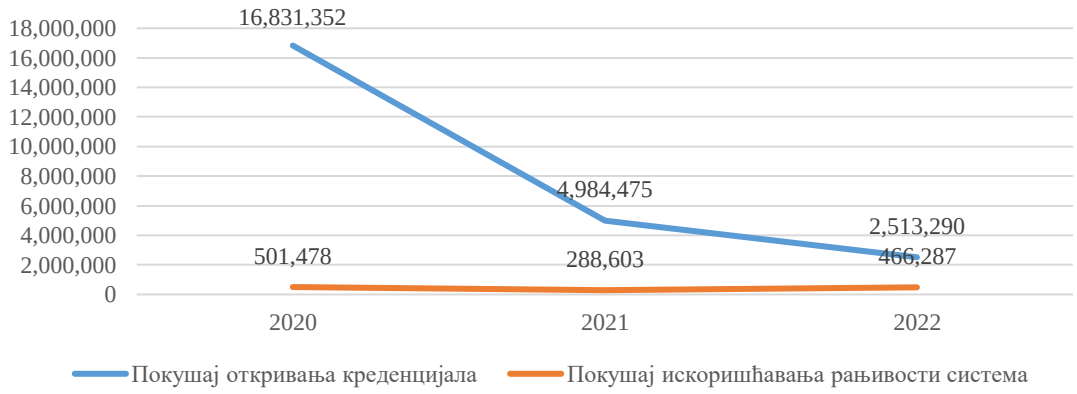
Неовлашћено прикупљање података обухвата социјални инжењеринг, компромитовање или цурење података, пресретање података између рачунара и сервера и скенирање портова. На дијаграмима се може приметити индикативни тренд повећања броја напада из ове групе, осим скенирања портова. Социјални инжењеринг је у 2020. и 2021. години био на релативно блиском нивоу, да би у 2022. години било регистровано преко четири пута више оваквих инцидената. Компромитовање или цурење података је имало велики скок у броју пријава 2021. у односу на 2020. годину и тај број се задржао и у 2022. години, док је број регистрованих случајева пресретања података између рачунара и сервера имао енорман раст са мање од 10 забележених случајева у 2020. и 2021. години, на преко 600 случајева у 2022. години.

Пријављени случајеви скенирања портова приказани су на посебном дијаграму због несразмерне разлике у броју у односу на друге врсте инцидената из ове групе, али ово је и једини пример у овој групи да постоји константан опадајући тренд. Овако велики број забележених случајева

последица је аутоматизованих процеса за испитивање доступних сервиса на удаљеним рачунарима, што не мора нужно бити вођено малициозним намерама али се врши без експлицитне сагласности оператора ИКТ система.

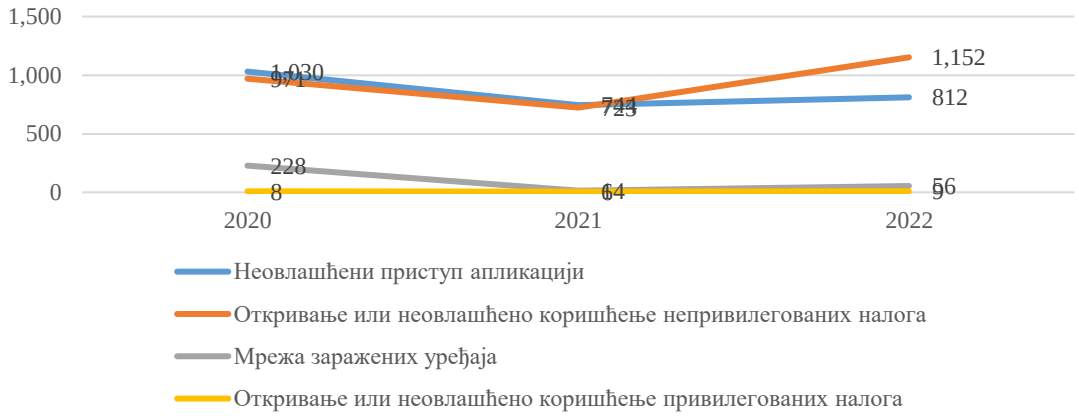
Дијаграм 10 Инциденти у групи Превара

У групи Превара налазе се фишинг и неовлашћено коришћење ресурса и други облици превара. Слично као код других типова инцидената који обухватају методе социјалног инжењеринга, и код фишинга је у 2021. години дошло до пада броја забележених случајева, да би у 2022. години број пријава драстично порастао. Сличан тренд може се видети и за друге случајеве неовлашћеног коришћења ресурса (као што је криптоцекинг) али у мањем броју и са процентуално мањим осцилацијама.



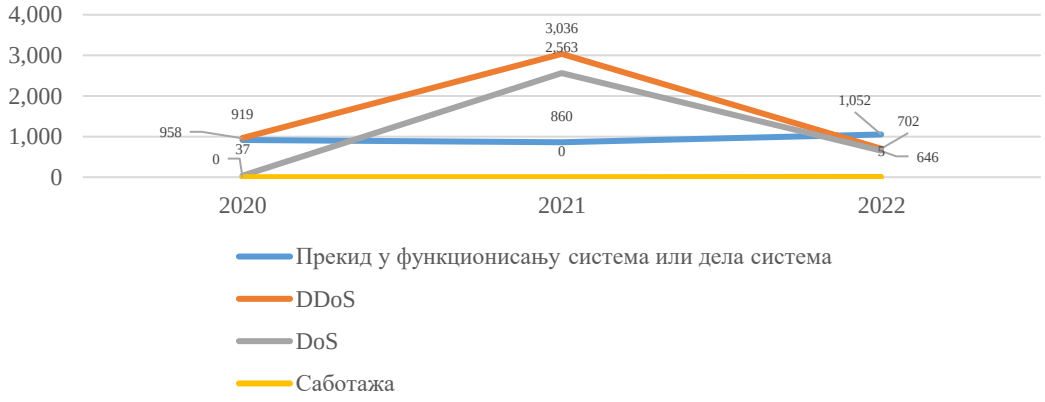
Дијаграм 11 Инциденти у групи Покушај упада у ИКТ систем

Да би упали у неки ИКТ систем нападачи покушавају да открију валидне креденцијале или да искористе рањивости система. За откривање креденцијала најчешће се примењују технике бруталне силе или речника које подразумевају да нападачи покушавају да се пријаве на систем са креденцијалима које уносе редом према одређеном шаблону све док не унесу исправан, што подразумева огроман број покушаја и зато су ови бројеви овако велики (мада се уочава тренд опадања броја покушаја). Други тип инцидента у овој групи, искоришћавање рањивости система, такође показује већ виђен трен да после смањења броја пријава у 2021. години долази до поновног повећања у 2022. години и враћања приближно на ниво из 2020. године.



Дијаграм 12 Инциденти у групи Упад у ИКТ систем

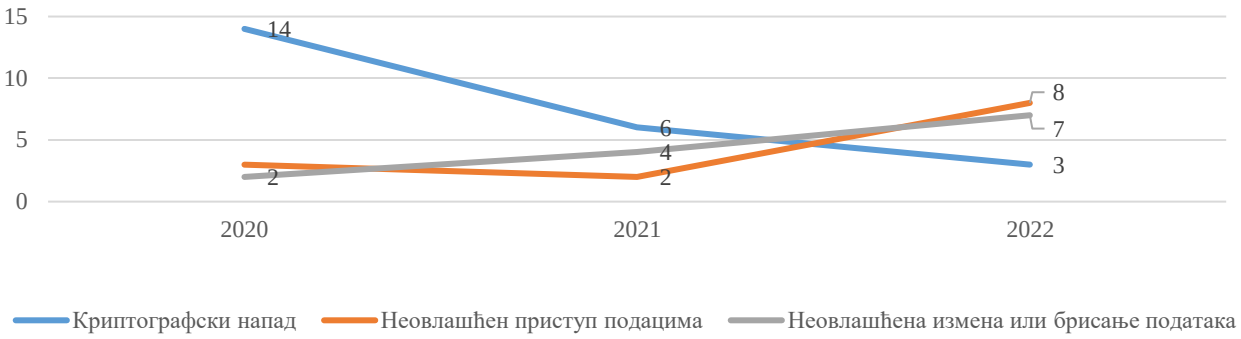
Неовлашћени приступ апликацији, откривање или неовлашћено коришћење непривилегованих налога, откривање или неовлашћено коришћење привилегованих налога и мрежа заражених уређаја су врсте инцидената које припадају групи Упад у ИКТ систем. У овој групи у 2022. години пријављено је највише откривања или неовлашћеног коришћења непривилегованих налога, са трендом да је забележен пад броја пријављених случајева 2021. године у односу на претходну годину и раст 2022. године.



Дијаграм 13 Инциденти у групи Недоступност или ограничена доступност ИКТ система

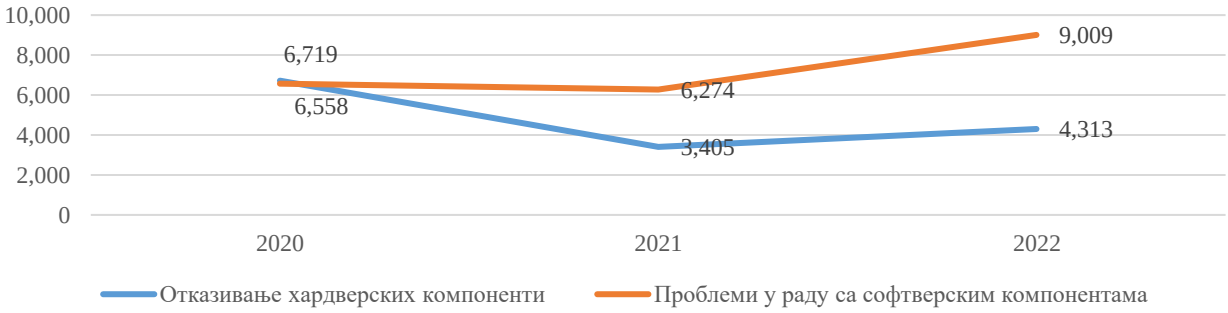
Неовлашћено откривање или коришћење привилегованих налога, које представља много озбиљнији инцидент јер у случају успешности нападачи имају могућност приступа осетљивим подацима, забележено је у приближно истом броју све три године.

Група Недоступност или ограничена доступност ИКТ система укључује четири типа инцидента: прекид у функционисању система или дела система (енг. *outage*), дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система (енг. *distributed denial-of-service - DDoS*), напад са циљем онемогућавања или ометања функционисања ИКТ система (енг. *Denial-of-Service - DoS*) и саботажу. За DoS и DDoS нападе приметан је обрнут тренд у односу на претежан тренд код других врста напада, у смислу да је у 2021. години уочен нагли скок броја пријављених напада, а у 2022. години нагли пад у односу на претходну годину. Такође се може уочити да у 2020. и 2021. години није забележен нити један случај саботаже, док је у 2022. години пријављено пет таквих случајева.



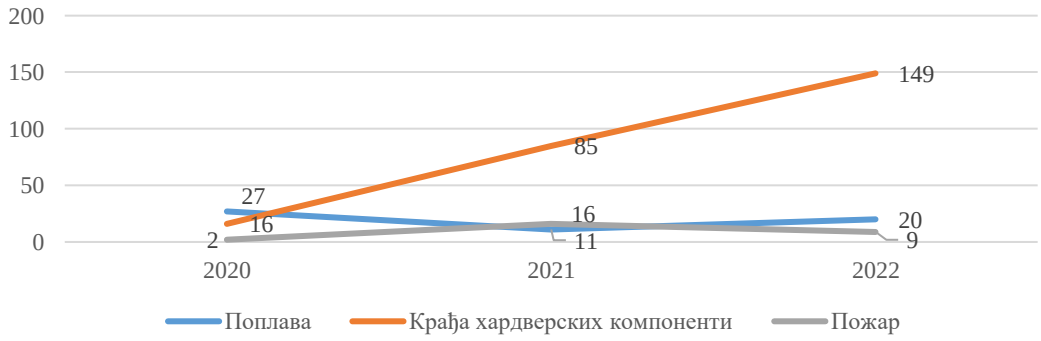
Дијаграм 14 Инциденти у групи Угрожавање безбедности података

Угрожавање безбедности података обухвата криптографски напад, неовлашћен приступ подацима и неовлашћене измене или брисање података. Укупан број ових напада није велики, а може се приметити благи тренд раста броја случајева неовлашћеног приступа подацима и неовлашћене измене или брисања података и тренд пада броја криптографских напада.



Дијаграм 15 Инциденти у групи Оперативни инциденти

Оперативни инциденти су они који доводе до застоја у пружању услуга, односно прекида који на било који начин угрожавају пословни процес изазваних отказивањем хардверских компоненти или проблема у раду са софтверским компонентама. У 2020. години број забележених проблема са хардверским и са софтверским компонентама био је приближно исти, док је у последње две године пријављен приближно двоструко већи број проблема са софтверским компонентама него са хардвером.



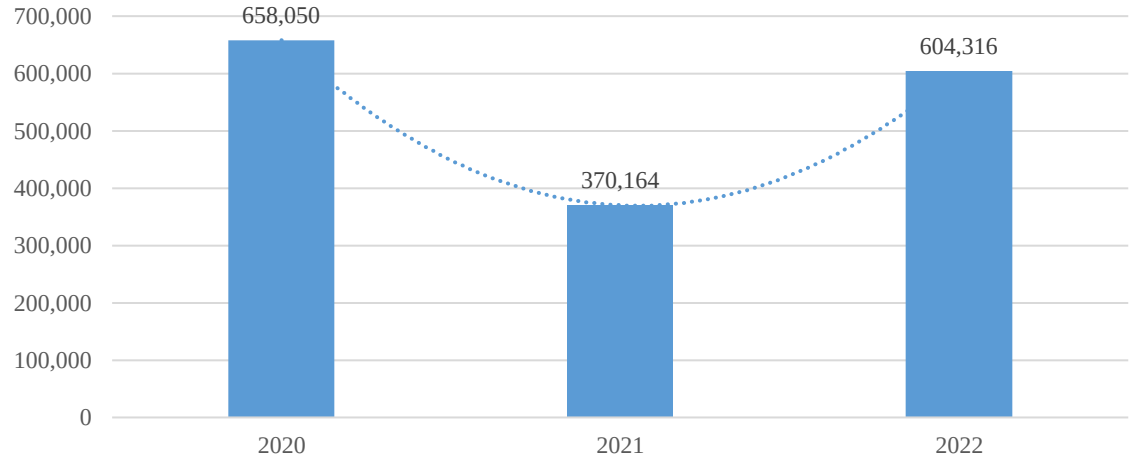
Дијаграм 16 Инциденти у групи Инциденти физичко-техничке безбедности

У групу Инцидената физичко-техничке безбедности спадају поплаве, пожари и крађе. Може се констатовати да је збир пожара и поплава у збиру прилично константан (по 29 у 2020. и 2022.

години и 27 у 2021. години), али је број пријављених крађа практично једини тип инцидента који бележи линеарни тренд раста у протекле три године.

У остале инциденте сврстани су сви они који не спадају у наведене категорије, као што су детекција потенцијално небезбедних апликација, неодобрене платне трансакције или лажни профили на друштвеним мрежама.

Укупан број пријављених инцидената у 2020. години био је 25.958.850, у 2021. години 13.279.007, а у 2022. години 10.808.838. Гледајући само ове бројеве могао би се стећи утисак да постоји генералан тренд смањења броја инцидената. Међутим, треба имати у виду да је у 2020. години број инцидената на глобалном нивоу еруптирао као последица пандемије и измењених околности пословања па ни Србија није била изузета од тог тренда (на жалост, статистика која би показала овај скок није вођена у Србији пре 2020. године). Следећа година донела је значајно смиривање, па поређење 2021. и 2022. године може боље показати прави тренд. Посматрајући тренд пријављених скенирања портова (8.469.448 у 2020. години, 7.924.368 у 2021. години и 7.691.232 у 2022. години) и број покушаја откривања креденцијала (16.831.352 у 2020. години, 4.984.475 у 2021. години и 2.513.290 у 2022. години) очигледно је да ове две врсте инцидената, које у свакој од ове три године заједно чине између 94,4% и 97,4% од укупног броја инцидената, бележе значајно смањење након прве године пандемије и требају бити третиране засебно због своје процентуалне заступљености. Ако се из укупног броја инцидената изузму ове две врсте, добија се следећи дијаграм броја инцидената по годинама:



Дијаграм 17 Укупан број инцидената по годинама без скенирања портова и покушаја откривања креденцијала

Ако се узме у обзир да је 2020. година била специфична и узме у обзир однос броја инцидената у 2021. и 2022. години, уочава се значајан и забрињавајући раст. На глобалном нивоу, прогнозе су да ће број инцидената значајно расти у наредном периоду (није нам позната нити једна анализа која закључује да ће број инцидената опадати), али такође и њихова софистицираност. Посебно су алармантна предвиђања да ће се наставити тренд раста просечне штете по инциденту, што значи да ће укупна сума штете нанете инцидентима расти у доста већем проценту од раста броја инцидената. Овакви трендови неће мимоићи ни Србију па се може очекивати да се и у наредним годинама настави раст броја пријављених инцидената, али и раст нанете штете.

2) Да ли се у предметној области спроводи или се спроводио документ јавне политике или пропис? Представити резултате спровођења тог документа јавне политике или прописа и образложити због чега добијени резултати нису у складу са планираним вредностима.

Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године представља међусекторску стратегију којом се утврђују циљеви и мере за развој информационог друштва и информационе безбедности. У делу који се односи на информациону безбедност Стратегија је усклађена са Директивом о мрежној и информационој безбедности ЕУ (енг. *Network and Information Security Directive - NIS Directive*), која предвиђа обавезу доношења националне стратегије за информациону безбедност којом ће се дефинисати стратешки циљеви и приоритети који се односе на мрежну и информациону безбедност.

Стратегијом је дефинисан посебан циљ ***Унапређење информационе безбедности грађана, јавне управе и привреде***, који се остварује кроз реализацију следећих мера:

- подизање свести и знања у области информационе безбедности грађана, јавних службеника и привреде,
- подизање капацитета ИКТ система од посебног значаја за примену мера заштите,
- подизање капацитета Националног ЦЕРТ-а, ЦЕРТ-а органа власти и ЦЕРТ-ова самосталних оператора ИКТ,
- подизање капацитета инспекције за информациону безбедност,
- подстицање јавно-приватног партнерства у области информационе безбедности и
- унапређење регионалне и међународне сарадње.

Акциони план за реализацију Стратегије развоја информационог друштва и информационе безбедности за период од 2024. до 2026. године мери оствареност овог посебног циља кроз Глобални индекс информационе безбедности (енг. *Global Cyber Security Indeks*) који мери осам индикатора: позицију државе у глобалним оквирима у овој области, индекс безбедности у сајбер простору, законе, техничку развијеност, организацију, капацитете, сарадњу и позицију државе у регионалним оквирима у овој области. У последњем издању „Глобалног индекс информационе безбедности“, Република Србија нашла се у првој од пет група држава која обухвата земље са највишим нивоом развоја у области информационе безбедности. Међународна телекомуникациона унија вредновала је пет кључних компоненти развоја, и то правни оквир, техничке мере, организационе мере, јачање капацитета и међународну сарадњу. Република Србија препозната је као једна од водећих земаља у свим овим аспектима чиме је потврђен значајан допринос наше земље у осигуравању високог нивоа информационе безбедности.

У оквиру мере *Подизање свести и знања у области информационе безбедности грађана, јавних службеника и привреде* реализоване су следеће активности:

- У сарадњи са надлежним Министарством креиране су и спроведене две врсте обука намењене представницима министарстава. Теоријску обуку под називом „Примена Модела акта о безбедности” похађало је укупно 27 запослених лица из 9 министарстава, а дводневну техничку обуку „Детекција и одбрана ИКТ система од сајбер напада” похађало је укупно 28 запослених из 8 министарстава. Такође, у сарадњи са Институтом за стандардизацију и Министарством унутрашњих послова одржан је вебинар под називом „Од ЗИБ-а до стандарда” намењен представницима судства и правосудних органа, који је похађало укупно 78 учесника.
- У сарадњи са Радио телевизијом Србије организована је медијска кампања намењена подизању свести о значају информационе безбедности у оквиру које су емитовани едукативни спотови на тему безбедности деце на интернету. Такође је у 10 епизода реализована и емисија „Породична мрежа” у циљу подизања свести о значају информационе безбедности, о ризицима и мерама заштите, у којој су активно учешће имали родитељи са децом.

- У току 2022. године спроведен је Јавни позив за доделу средстава за организовање регионалних конференција на тему размене искуства у области подизања нивоа дигиталне писмености, дигиталних компетенција и реализацију програма који за циљ имају подизање дигиталних компетенција жена из руралних области.
- Израђен је Водич за сајбер безбедност малих и средњих предузећа у сарадњи са Националним ЦЕРТ-ом Републике Србије. Водич је намењен малим и средњим предузећима и садржи упутства о томе како се заштитити од најчешћих претњи по информациону безбедност с којима мала и средња предузећа могу да се сусретну у свом раду, а заснован је на доказаним примерима добре праксе приватног и јавног сектора.
- Национални ЦЕРТ Републике Србије креирао је платформу за подизање свести и знања из области информационе безбедности, која је доступна на адреси: https://learn.cert.rs/Home/Home?mostrarTour=True.

У оквиру мере *Унапређење сарадње и подизање капацитета ИКТ система од посебног значаја за примену мера заштите*:

- одржане су обуке и вежбе за представнике правосудних органа и оператора ИКТ система од посебног значаја у области енергетике;
- припремљене су смернице за достизање неопходног нивоа испуњености захтева (енг. *common criteria*) за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;
- у октобру 2022. године од стране Регулаторне агенције за електронске комуникације и поштанске услуге (РАТЕЛ), као Националног ЦЕРТ-а, организована је Национална конференција „Будимо сајбер свесни", којом је обележен октобар као међународни месец информационе безбедности на којој су презентована актуелна дешавања у сајбер простору, начини унапређења сарадње и размене информација о сајбер претњама, представљени су начини заштите критичне инфраструктуре, као и значај јавно-приватног партнерства у овој области;
- током новембра 2022. године одржана је конференција у организацији Регистра националног Интернет домена Србије на којој су настављени разговори поводом подизања свести и едукације о информационој безбедности и презентовани су резултати пројеката Сајбер херој и дигиталне кампање Заштити се;
- у оквиру базе Националног ЦЕРТ-а креиран је део за размену података између Националног ЦЕРТ-а и ИКТ система од посебног значаја и успостављена је платформа за размену података *MISP - Malware Information Sharing Platform*);
- у току је припрема образаца за самопроцену ИКТ система од посебног значаја као и за проверу степена развијености информационе безбедности у Републици Србији.

У оквиру мере *Подизање капацитета Националног ЦЕРТ-а, ЦЕРТ-а органа власти и ЦЕРТ-ова самосталних оператора ИКТ система*:

- израђене су смернице за поступање у случају инцидената који су високог и веома високог нивоа опасности;
- успостављена је сарадња између Министарства, Националног ЦЕРТ-а и Сектора за ванредне ситуације у оквиру Министарства унутрашњих послова ради препознавања механизама сарадње у случају инцидента веома високог нивоа опасности;
- успостављен је ЦЕРТ Министарства одбране и уписан у Евиденцију ИКТ система од посебног значаја;
- континуирано се врши похађање обука запослених у Националном ЦЕРТ-у у складу са планом стручног усавршавања РАТЕЛ-а

Подизање капацитета инспекције за информациону безбедност врши се кроз бројне обуке међу којима су најзначајније:

- Обука коју је организовало Акредитационо тело Србије уз учешће ЕУ експерата везано за eIDAS регулативу (енг. *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*);
- Обуке за коришћење софтвера еИнспектор;
- Учествовање на Техничком колоквијуму за ЦЕРТ-ове Западног Балкана коју је организовао Женевски центар за управљање безбедносним сектором (енг. *Geneva Centre for Security Sector Governance - DCAF*) у сарадњи са Албанском националном агенцијом за електронску сертификацију и информациону безбедност (AKCESK) у оквиру регионалног пројекта;
- Обука Института за стандардизацију за чланове комисија за стандарде и сродне документе;
- NFC радионица коју је организовала Агенција Европске Уније за сајбер безбедност – ЕНИСА.

Мера *Подстицање јавно-приватног партнерства у области информационе безбедности* реализује се кроз следеће активности:

- У оквиру фондације „Мрежа за сајбер безбедност" (некадашња Петничка група), која повезује привреду и доносиоце одлука о политикама кроз платформу за дискусију и спровођење активности усмерених ка унапређењу информационе безбедности у Србији, реализује се програм „Сајбер херој" у оквиру кога се реализује такмичење у области информационе безбедности *Serbian Cybersecurity Challenge*. 2022. године национални тим Србије учествовао је на међународном такмичењу *European Cyber Security Challenge* (ЕЦСЦ 2022). Поред тога, на позив Агенције Европске Уније за сајбер безбедност – ЕНИСА, два представника из Србије били су кандидати за Тим Европе на такмичењу континената.
- Закључени су споразуми о сарадњи са Савезом слепих Београд и Савезом глувих Београд - постигнут је договор о одржавању презентација на тему безбедности деце на интернету.

Унапређење регионалне и међународне сарадње спроводи се кроз бројне активности предвиђене акционим планом међу којима се издвајају:

- У оквиру иницијативе „Отворени Балкан" закључен је Споразум о повезивању шема електронске идентификације грађана Западног Балкана између Србије, Албаније и Северне Македоније, чиме су државе међусобно признале шеме електронске идентификације уписане у одговарајуће регистре. Закључивање овог споразума подразумева да стране технички повежу своје портале електронске управе тако да грађани могу да се електронски идентификују у складу са најнапреднијим стандардима информационе безбедности.
- У септембру 2022. године потписан је Меморандум о разумевању у области информационе безбедности између Министарства информисања и телекомуникација Републике Србије и Савета за сајбер безбедност Уједињених Арапских Емирата. Сарадња предвиђена овим меморандумом се спроводи кроз разне унапред договорене форме, укључујући обуку, техничке консултације и размену стручњака у неопходним областима. Области сарадње предвиђене меморандумом су: размена информација о ризицима по информациону безбедност, заједничко информисање и одговор на инциденте на пољу информационе безбедности, подела информација о ширењу злонамерних софтвера, размена података о индикаторима компромитације, пружање информација о могућим успешним решењима у области информационе безбедности, заједничка сарадња у организовању техничких

радионица, конференција, едукативних посета и обука, заједничка координација и сарадња у организацији и спровођењу обука у области информационе безбедности.

- У новембру 2022. године у Београду реализована је *TAIEX* експертска мисија које се односи на сертификацију у области информационе безбедности, као и на остала питања у вези са применом Акта о сајбер безбедности ЕУ (Уредба 2019/881). TAIEX је инструмент Европске комисије за техничку помоћ и размену информација и подржава јавну администрацију у вези са усклађивањем, применом и спровођењем законодавства ЕУ, као и олакшавањем размене најбољих пракси ЕУ. Експертској мисији присуствовали су представници Канцеларије за информационе технологије и електронску управу, Министарства одбране, Министарства информисања и телекомуникација, Безбедносно – информативне агенције, као и представници РАТЕЛ-а - Националног ЦЕРТ-а. Експертска мисија затражена је у циљу припреме за ревидирање прописа из области информационе безбедности у складу са најновијим законодавством ЕУ.
- У октобру 2022. године одржан је семинар о Предлогу НИС 2 директиве Европске уније, упоредној пракси у вези уређења и рада агенција за информациону безбедност, променама у стандарду ИСО 27001 и најбољим решењима у погледу управљања кризним ситуацијама у случају сајбер инцидената. У вези са наведеним темама учесници семинара представили су правни и стратешки оквир и праксу из свог делокруга рада.
- У октобру 2022. године Министарство је учествовало на међународној конференцији *INSAFE AND INHOPE*, одржаној у Бриселу.
- Надлежни органи РС сарађују са ЕУ институцијама надлежним за област информационе безбедности. Министарство остварује сарадњу са Међународном унијом за телекомуникације у погледу израде Глобалног индекса сајбер безбедности, као и са Агенцијом Европске Уније за сајбер безбедност ЕНИСА учешћем у радној групи за електронску идентификацију и квалификоване услуге од поверења. ЦЕРТ-ови из Републике из Србије налазе се на *Trusted Introducer* листи, а Национални ЦЕРТ и ЦЕРТ МУП чланови су *Forum of Incident Response and Security Teams* организације.

И поред успешног спровођења активности предвиђених Стратегијом развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године, због недовољних кадровских и техничких капацитета надлежних органа у области информационе безбедности, касни се у реализацији појединих активности, као што су: израда смерница за достизање неопходног нивоа испуњености захтева (енг. *common criteria*) за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система; развој, хармонизација и проширење специјализованих курсева и програма информационе безбедности на универзитетима и другим високошколским установама; обуке за мала и средња предузећа о потреби и начину примене мера заштите и важности континуираног подизања капацитета запослених, у складу са националним и међународним стандардима. Због измена европских директива у овој области неопходно је извршити хармонизацију прописа и ускладити одредбе Закона о информационој безбедности са НИС 2 Директивом (енг. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 - NIS 2 Directive)* Усклађивање прописа омогућиће наставак сарадње са међународним телима и испуњење обавеза Републике Србије у процесу придруживања Европској унији. Унапређење правног оквира требало би да побољша не само међународну сарадњу, већ и капацитете свих ентитета надлежних за обезбеђивање информационе безбедности.

3) Да ли су уочени проблеми у области и на кога се они односе? Представити узроке и последице проблема.

Анализирајући постојећи законски оквир и његову имплементацију, циљеве постављене Стратегијом развоја информационог друштва и информационе безбедности за период 2021.-2026. године и правце развоја на глобалном и нивоу Европске уније, могу се идентификовати следећи проблеми који се могу превазићи искључиво изменом институционалног и правног оквира:

- неусклађеност Закона о информационој безбедности са европским прописима,
- недостатак капацитета надлежних органа,
- потреба за подизањем оперативних капацитета за реаговање на инциденте, посебно на оне од националног значаја,
- недостатак системског прикупљања и размене информација,
- непостојање националне платформе за брзу детекцију инцидената,
- недостатак координације за откривање рањивости и
- недовољна координација међународних активности.

Неусклађеност Закона о информационој безбедности са европским прописима

Измене и допуне Закона о информационој безбедности 2019. године односиле су се на усклађивање са НИС Директивом која је у децембру 2022. године замењена НИС 2 Директивом.

Због тога је представљена упоредна анализа НИС и НИС 2 Директиве, како би се препознале разлике у правном оквиру које је неопходно превазићи. НИС Директива уводи 19 дефиниција, док је у НИС 2 Директиви овај број порастао на 41. Већина дефиниција из НИС Директиве задржана је и у НИС 2 Директиви у истом или практично истом облику, али је неколико дефиниција термина претрпело суштинске промене.

На пример, термин „инцидент" је у НИС Директиви дефинисан као било који догађај који има стварни нежељени ефекат на безбедност мрежних и информационих система, док је у НИС 2 Директиви овај термин дефинисан као догађај који компромитује доступност, аутентичност, интегритет или поверљивост складиштених, преношених или процесираних података, или услуга које се нуде или којима се приступа путем мрежних и информационих система. Дефиниција термина „руковање инцидентом" у НИС 2 Директиви проширена је превенцијом, реаговањем и опоравком, уз детекцију, анализу и ограничавање који су већ били укључени у дефиницију овог термина у НИС Директиви.

НИС Директива је у свом члану 5 прописивала критеријуме за одређивање оператора есенцијалних сервиса:

- ентитет пружа сервис који је неопходан за одржавање критичних друштвених и/или економских активности;
- пружање тог сервиса зависи од мрежних и информационих система; и
- инцидент би имао значајне реметилачке ефекте на пружање тог сервиса.

Ови критеријуми нису задржани у НИС 2 Директиви, већ је ова Директива ентитете којима су прописане посебне обавезе поделила на есенцијалне и важне. У складу са овом поделом, одређени су и сектори високе критичности и остали критични сектори у којима се обављају делатности од посебног значаја. НИС 2 Директивом одређено је да у секторе високе критичности спадају:

- енергетика,
- саобраћај,
- банкарство,
- инфраструктуре финансијских тржишта,

- здравље,
- пијаћа вода,
- отпадне воде,
- дигитална инфраструктура,
- управљање ИКТ услугама,
- јавна администрација и
- свемир.

Уређено је да у остале критичне секторе спадају:

- поштанске и курирске услуге,
- управљање отпадом,
- производња и снабдевање хемикалијама,
- производња, обрада и дистрибуција хране,
- друге производне делатности (производња медицинских уређаја и in vitro дијагностичких медицинских средстава, рачунара, електронских и оптичких производа, електричне опреме, машина и уређаја, моторних возила, приколица и полуприколица и производња остале опреме за превоз),
- пружање дигиталних услуга и
- истраживање.

Одредбама НИС 2 Директиве прописано је да се есенцијалним ентитетима сматрају:

- ентитети који превазилазе величину средњих предузећа (имају више од 250 запослених и обрт од преко 50 милиона евра) и који своју делатност обављају у неком од високо критичних сектора;
- пружаоци квалификованих услуга од поверења, пружаоци услуге регистрације домена највишег нивоа и пружаоци услуга DNS без обзира на величину;
- пружаоци услуга јавних електронских комуникационих мрежа или јавно доступних електронских комуникационих услуга који спадају у предузећа средње величине;
- органи државне управе на централном нивоу;
- сви други ентитети који своје делатности обављају у високо критичним или критичним секторима, а које је држава чланица идентификовала као есенцијалне јер су једини пружаоци неке есенцијалне услуге, јер би прекид у пружању услуга могао имати значајан утицај на јавну сигурност, јавну безбедност и јавно здравље, јер би прекид у пружању услуга могао имати значајан системски ризик, или који су критични због специфичне важности на националном или регионалном нивоу;
- ентитети идентификовани као критични у складу са Директивом 2022/2557;
- сви други ентитети идентификовани као есенцијални у складу са Директивом 2016/1148 (НИС Директива), ако држава чланица процени да је то потребно.

Важним ентитетима сматрају се ентитети који своје делатности обављају у високо критичним или критичним секторима, а који не испуњавају критеријуме да буду идентификовани као есенцијални. Такође, важним ентитетима се сматрају и они које је држава чланица идентификовала као важне јер су једини пружаоци неке есенцијалне услуге, јер би прекид у пружању услуга могао имати значајан утицај на јавну сигурност, јавну безбедност и јавно здравље, јер би прекид у пружању услуга могао имати значајан системски ризик, или који су критични због специфичне важности на националном или регионалном нивоу.

НИС директивом прописано је да се одређивање шта представља значајан реметилачки ефекат препусти земљама чланицама, при чему је Директивом сугерисано да се у обзир узме:

- број корисника сервиса који пружа тај ентитет који су погођени прекидом;
- зависност других сектора којима припадају оператори есенцијалних сервиса од сервиса који пружа тај ентитет;

- утицај који би инциденти могли имати, у смислу обима и трајања, на економске и друштвене активности или јавну безбедност;
- тржишни удео тог ентитета;
- географско ширење у погледу подручја које би могло бити погођено инцидентом; и
- важност ентитета за одржавање довољног нивоа сервиса, узимајући у обзир доступност алтернативних могућности за пружање тог сервиса.

У НИС 2 Директиви није задржан појам значајног реметилачког ефекта, али су уведени појмови значајне сајбер претње и значајног инцидента. Значајна сајбер претња је као појам дефинисана у члану 3. НИС 2 Директиве као сајбер претња за коју се, на основу својих техничких карактеристика, може претпоставити да има потенцијал да озбиљно утиче на мрежне и информационе системе ентитета или кориснике његових услуга наношењем знатне материјалне или нематеријалне штете. Чланом 23, којим су прописане обавезе извештавања, дефинисано је да ће се инцидент сматрати значајним ако:

- је проузроковао или има капацитет да проузрокује озбиљне прекиде пружања услуга или озбиљне финансијске губитке угроженом ентитету, и
- је утицао или има капацитет да утиче на друга физичка или правна лица путем наношења значајне материјалне или нематеријалне штете.

НИС Директива обавезала је државе чланице да усвоје националну стратегију безбедности мрежних и информационих система која мора укључивати следеће:

- циљеве и приоритете националне стратегије безбедности мрежних и информационих система;
- оквир управљања за постизање циљева и приоритета ове стратегије, укључујући улоге и одговорности државних органа и других релевантних актера;
- утврђивање мера које се односе на припремљеност, реаговање и опоравак, укључујући сарадњу између јавног и приватног сектора;
- програме образовања, подизања свести и обуке;
- планове истраживања и развоја;
- план процене ризика ради њихове идентификације;
- списак актера укључених у спровођење националне стратегије безбедности мрежних и информационих система.

У НИС 2 Директиви такође постоји обавеза за државе чланице да усвоје националну стратегију (али се користи израз „национална стратегија информационе безбедности”), при чему је списак обавезних ставки остао сличан, а додате су и координација и сарадња. Такође, државама чланицама је дата обавеза да као део националне стратегије усвоје следеће политике:

- решавање информационе безбедности у ланцу снабдевања;
- укључивање и спецификацију захтева везаних за безбедност ИКТ производа и услуга у јавним набавкама;
- управљање рањивостима;
- одржавање опште доступности, интегритета и поверљивости јавног језгра отвореног интернета;
- промовисање развоја и интеграције релевантних напредних технологија са циљем имплементације најсавременијих мера за управљање ризиком у области информационе безбедности;
- промовисање и развој образовања и обука, вештина, подизања свести и иницијатива за истраживање и развој, као и смерница о добрим праксама и контролама сајбер хигијене;

- подршка академским и истраживачким институцијама у развоју, унапређењу и промоцији примене алата за информациону безбедност;
- подршка добровољној размени информација;
- јачање сајбер отпорности и основе сајбер хигијене малих и средњих предузећа;
- промовисање активне сајбер заштите.

Обе директиве прописују обавезе за државе чланице да одреде надлежне органе (један или више) и јединствену тачку контакта, као и да успоставе Тимове за хитно реаговање на инциденте - ЦСИРТ (енг. *Computer emergency response team*) са надлежностима које покривају секторе од посебног значаја.

НИС 2 Директивом задржане су одредбе о Групи за сарадњу и Мрежи ЦСИРТ-ова из НИС Директиве, уз нешто проширен скуп задатака за ова два тела.

НИС 2 Директивом детаљније су разрађене техничке, оперативне (додатна врста мера која није била поменута у НИС Директиви) и организационе мере за управљање ризицима по мрежне и информационе системе. У ове мере спадају:

- политике у вези анализе ризика и безбедности информационих система;
- руковање инцидентима;
- континуитет пословања и управљање кризама;
- безбедност ланца снабдевања;
- безбедност у набавци, развоју и одржавању мрежних и информационих система, укључујући откривање и руковање рањивостима;
- политике и процедуре за процену ефикасности мера за управљање ризиком;
- практиковање основних мера сајбер хигијене и обуке у циљу подизања безбедносне свести;
- политике и процедуре везане за коришћење криптографских метода;
- безбедност људских ресурса, политике контроле приступа и управљање асетима;
- коришћење мултифакторске аутентификације и других метода јаке аутентификације и коришћење безбедних комуникационих система, посебно у случају ванредних ситуација.

НИС 2 Директива задржала је одредбе о обавези извештавања о инцидентима, при чему се ова обавеза односи и на есенцијалне и на важне ентитете.

У односу на НИС Директиву, у новој Директиви уведена је обавеза за државе чланице да одреде или успоставе један или више надлежних органа одговорних за управљање великим инцидентима и кризама. Ако се одреди више органа, мора се недвосмислено одредити која институција координира њихов рад у случају великих инцидената и криза. Државе чланице такође морају усвојити национални план за одговор на велике инциденте и кризе који мора садржати:

- циљеве због којих се предузимају мере и активности,
- задатке и одговорности надлежних органа,
- процедуре за реаговање и њихово уклапање у општи оквир за реаговање у случају националне кризе, као и канале за размену информација,
- мере које је потребно предузети ради припреме, укључујући вежбе и обуке,
- организације из јавног и приватног сектора и инфраструктуру која се ангажује,
- процедуре и споразуме између националних надлежних органа.

НИС 2 Директивом прописани су слични захтеви и проширен скуп задатака за ЦСИРТ-ове (ЦЕРТ-ове) у односу на НИС Директиву. Додатни захтев у НИС 2 Директиви је да су ЦСИРТ-ови у обавези да обезбеде поверљивост и поузданост својих операција, а задаци за ЦСИРТ-ове су следећи:

- праћење и анализирање сајбер претњи, рањивости и инцидената на националном нивоу и, на захтев, пружање помоћи есенцијалним и важним ентитетима,
- пружање раних упозорења и других информација о ризицима и инцидентима есенцијалним и важним ентитетима, надлежним органима и другим субјектима од значаја,
- реаговање на инциденте и пружање помоћи есенцијалним и важним ентитетима (где је применљиво),
- пружање динамичке анализе ризика и инцидената и указивање на тренутну ситуацију,
- пружање есенцијалним и важним ентитетима услуге проактивног скенирања мрежних и информационих система ради откривања рањивости,
- учешће у Мрежи ЦСИРТ-ова,
- координација активности усмерених на координисано откривање рањивости (где је применљиво), и
- допринос примени безбедних алата за размену информација.

Одредбе о координисаном откривању рањивости су уведене у НИС 2 Директиву као нова тема (која није постојала у НИС Директиви). НИС 2 Директивом прописано је да државе чланице треба да одреде ЦСИРТ који ће бити координатор ових активности. Тај ЦСИРТ треба да делује као посредник од поверења и олакша комуникацију између оног ко пријављује рањивост (било да је у питању правно или физичко лице) и произвођача потенцијално рањивог производа или пружаоца потенцијално рањиве услуге. Задаци овог ЦСИРТ-а укључују:

- идентификацију и успостављање контакта са предметним странама,
- помоћ страни која пријављује рањивост и
- договарање о роковима за објављивање, као и управљање рањивостима које утичу на више ентитета.

Страни која пријављује рањивост мора бити загарантована анонимност ако то жели.

НИС 2 Директива даје задатак ЕНИСА-и да развије и одржава Европску базу рањивости, укључујући одговарајући информациони систем, политике и процедуре, као и да предузме неопходне техничке и организационе мере које ће гарантовати безбедност и интегритет ове базе података. База података ће бити доступна свим значајним ентитетима, а садржаће следеће податке:

- опис рањивости,
- обухваћене производе или услуге и озбиљност рањивости у смислу околности под којима она може бити експлоатисана и
- доступност одговарајуће закрпе или упутство за умањење ризика ако закрпа не постоји.

Новитет у НИС 2 Директиви је успостављање Европске мреже за организацију везе за сајбер кризе (EU-CyCLONe). Сврха успостављања ове мреже је подршка управљању великим инцидентима и кризама на оперативном нивоу и осигурање размене релевантних информација између држава чланица и институција ЕУ. Задаци ове мреже су:

- да повећа ниво припремљености за управљање великим инцидентима и кризама;
- да развије заједничку свест о ситуацији у вези са великим инцидентима и кризама;
- да процени последице и утицај релевантних великих инцидената и криза и предложи мере за ублажавање;
- да координира управљање великим инцидентима и кризама и подржи доношење одлука на политичком нивоу у вези са њима;
- да расправља, на захтев државе чланице, о националним плановима за реаговање на велике инциденте и кризе.

Нови задатак који је ЕНИСА добила НИС 2 Директивом је да, у сарадњи са Европском Комисијом и Групом за сарадњу, изради извештај о стању у ЕУ у области информационе безбедности и да га представи Европском Парламенту. Овај извештај се израђује сваке друге године и треба да обухвати:

- процену ризика на нивоу ЕУ;
- процену развоја капацитета у области информационе безбедности у јавном и приватном сектору;
- процену општег нивоа свести о информационој безбедности и сајбер хигијени међу грађанима и ентитетима, укључујући мала и средња предузећа;
- збирну процену нивоа зрелости капацитета и ресурса за информациону безбедност широм ЕУ, као и степена до којег су усклађене националне стратегије информационе безбедности држава чланица.

Група за сарадњу је НИС 2 Директивом добила задатак да до 17. јануара 2025. године, уз помоћ Европске Комисије, ЕНИСА и Мреже ЦСИРТ-ова, успостави методологију и организационе аспекте партнерских прегледа (енг. *peer reviews*), са сврхом учења из туђих искустава, ојачавања узајамног поверења, постизања високог заједничког нивоа информационе безбедности и побољшања капацитета и политика држава чланица да имплементирају ову Директиву. Партнерски прегледи морају бити добровољни и спровођени од стране најмање два експерта у области информационе безбедности који нису из државе чланице у којој се врши преглед. Партнерски прегледи морају обухватити макар једну од следећих процена:

- ниво имплементације мера за управљање ризицима у информационој безбедности и имплементације обавеза у вези извештавања утврђених овом Директивом;
- ниво способности, укључујући расположиве финансијске, техничке и људске ресурсе, и ефикасност извршавања задатака;
- оперативне способности ЦСИРТ-ова;
- ниво имплементације узајамне помоћи;
- ниво имплементације размене информација;
- посебна питања прекограничне или међусекторске природе.

НИС 2 Директивом је прописано да државе чланице могу захтевати од есенцијалних и важних ентитета да користе одређене ИКТ производе, услуге и процесе, који су сертификовани према европским шемама сертификације за информациону безбедност усвојеним у складу са Актом о сајбер безбедности. Поред тога, Европска Комисија има овлашћења да допуни ову Директиву прецизирајући које категорије есенцијалних и важних ентитета треба да користе одређене сертификоване ИКТ производе, услуге и процесе. Ако одговарајућа европска шема сертификације за информациону безбедност није доступна, Европска Комисија може захтевати од ЕНИСА да припреми ову шему.

Због наведених измена правног оквира Европске уније ствара се јаз у прописима које Република Србија, не само због обавеза преузетих у процесу хармонизације и прикључења Европској унији, већ због унапређења саме области, мора да превазиђе. Стога је неопходно извршити усклађивање правног оквира и Закон о информационој безбедности хармонизовати са наведеном Директивом.

Недостатак капацитета надлежних органа

Током имплементације Закона утврђено је да ИКТ системи од посебног значаја не достављају информације о свим инцидентима који значајно угрожавају информациону безбедност, иако су обавезни да то чине. Услед тога Национални ЦЕРТ није у могућности да у потпуности прати

трендове у овој области, што има утицај и на анализе ризика и инцидената на основу којих би се пружали савети и предлагале мере за отклањања потенцијалних инцидената.

За испуњавање свих законом предвиђених надлежности неопходно је да Национални ЦЕРТ и остали ЦЕРТ-ови основани у Републици Србији имају адекватне ресурсе. Постоји генерално мишљење у стручној јавности да се област информационе безбедности не схвата довољно озбиљно и да се могуће последице од напада на ИКТ системе потцењују, односно не придаје им се довољна пажња. Једно од питања које се често поставља је могућност обезбеђења неопходних људских ресурса и адекватна накнада за њихов рад, имајући у виду ситуацију на тржишту са овим кадром насупрот ограничењима која намећу прописи у јавном сектору. У том контексту потребно је сагледати капацитете (пре свега кадровске али и организационо-техничке) надлежног органа (у даљем тексту: Министарство). Као и код других државних и осталих органа, и Министарство се суочава са проблемом да привуче и задржи довољно стручан кадар који ће се бавити информационом безбедношћу.

Проблем са кадровима се посебно односи на послове инспекције за информациону безбедност, односно на чињеницу да тренутно инспекција броји два инспектора. Законом о информационој безбедности предвиђено је да ова инспекција врши надзор над применом закона и над радом ИКТ система од посебног значаја. Имајући у виду број ИКТ система од посебног значаја јасно је да два инспектора не могу благовремено да спроведе надзор над већим бројем ИКТ система од посебног значаја. Законом је предвиђено да инспектор има овлашћења да наложи отклањање утврђених неправилности и да забрани коришћење поступака или техничких средстава којима се угрожава или нарушава информациона безбедност, као и да остави рок за примену наложених мера. С обзиром да је ово начин да се примене неке мере неопходне за сузбијање инцидената, у случају одсуства инспектора не постоји алтернативни начин за налагање тих мера.

Недостатак оперативних капацитета за реаговање на инциденте

У Републици Србији су у последњих неколико година развијани капацитети за реаговање на инциденте у неколико органа управе, али у већини организација, како у јавном сектору тако и генерално у онима које су надлежне за управљање ИКТ системима који припадају критичној инфраструктури, нема довољно изграђених капацитета, па углавном зависе од трећих лица. Национални ЦЕРТ реагује по пријављеним или на други начин откривеним инцидентима у ИКТ системима од посебног значаја, као и по пријавама физичких и правних лица, тако што пружа савете и препоруке на основу расположивих информација о инцидентима и предузима друге потребне мере из своје надлежности на основу добијених сазнања, док се надлежности ЦЕРТ-а органа власти у Канцеларији за информационе технологије и електронску управу односе, пре свега, на заштиту информационо-комуникационих система јединствене информационо-комуникационе мреже електронске управе.

Имајући ово у виду, чак ни законски није покривена оперативна помоћ другим ИКТ системима од посебног значаја, осим оних који се налазе у оквиру система електронске управе. У претходном периоду извршено је неколико озбиљних напада на ИКТ системе у јавном сектору у Србији (поменимо само нападе на ЈКП Информатика из Новог Сада и на Републички геодетски завод) који су захтевали ангажовање неких оперативних тимова из јавног сектора којима овакве интервенције нису у надлежности, али и специјализованих приватних компанија. Овакви примери јасно указују да постоји потреба за успостављањем оперативног тима који би имао надлежност, али и знање да оперативно реагује у случајевима инцидената у ИКТ системима од посебног значаја, када оператор угроженог ИКТ система нема сопствене капацитете за решавање инцидента.

Такође, један од идентификованих проблема је непостојање обавезних вежби на којима би се преиспитивале и увежбавале процедуре за реаговање у случају инцидента. Овакве вежбе су устаљена пракса у развијеним земљама, док се у Србији нису организовале у значајној мери. Изузетак су сајбер вежбе „Сајбер Тесла" које се од 2016. године у Републици Србији организују на годишњем нивоу у сарадњи Војске Србије и Националне гарде Охаја. У циљу подизања капацитета запослених у ЦЕРТ-овима у Републици Србији, укључујући и ЦЕРТ-ове самосталних оператора, у оквиру пројекта „Унапређење информационе безбедности на Западном Балкану" организоване су тренинзи и обуке. Један од идентификованих проблема приликом организације оваквих вежби је редован изостанак доносиоца одлука, односно делегирање ниже рангираних службеника у својству замене.

Недостатак системског прикупљања и размене информација

Национални ЦЕРТ има надлежност да прикупља и размењује информације о ризицима за безбедност ИКТ система, као и о догађајима који угрожавају безбедност ИКТ система и у вези тога обавештава, пружа подршку, упозорава и саветује лица која управљају ИКТ системима у Републици Србији, као и јавност. Национални ЦЕРТ је и тачка контакта са другим сличним организацијама ван Србије и са међународним организацијама и удружењима. У међународној пракси национални ЦЕРТ-ови добијају посебан положај и приступ информацијама у вези информационе безбедности које нису јавно објављене, како би могли да их дистрибуирају до субјеката којима су ове информације потребне. По овом питању Национални ЦЕРТ је већ спровео одређене активности, као што су оне на имплементацији MISP платформе. Ове активности свакако треба наставити али је потребно укључити већи број субјеката.

Пријава инцидената је један од важних облика прикупљања информација. Може се констатовати да се побољшава дисциплина по питању поштовања ове законске обавезе али се не може рећи да се она у потпуности поштује, јер је извесно да се многи инциденти не пријављују, а откривају се у медијима или путем других канала комуникације. Разлози за непријављивање су разни – необавештеност да је пријављивање обавезно, недовољна свест о значају пријављивања, страх од угрожавања репутације, заузетост другим пословима, или једноставна небрига. Потребно је у континуитету подстицати пријављивање инцидената, посебно ако би то обезбедило и одређени ниво приступа систему за размену информација.

Низак степен превенције и заштите ИКТ система од посебног значаја

Законом о информационој безбедности дефинисано је да су ИКТ системи од посебног значаја системи који се користе у обављању послова у органима власти, за обраду посебних врста података о личности, у обављању делатности од општег интереса и других делатности у одређеним секторима (енергетика, саобраћај, здравство, банкарство и финансијска тржишта, дигитална инфраструктура, добра од општег интереса, услуге информационог друштва и остале области) и у правним лицима и установама које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе за обављање претходно наведених делатности.

ИКТ системи од посебног значаја по овом Закону имају обавезу да се упишу у евиденцију оператора ИКТ система од посебног значаја, предузму мере заштите овог система, донесу акт о безбедности, врше периодичну проверу усклађености примењених мера заштите са усвојеним актом о безбедности, уреде однос са трећим лицима у складу са законом ако њима поверавају активности у вези са ИКТ системом од посебног значаја, достављају обавештења о инцидентима који значајно угрожавају информациону безбедност ИКТ система и достављају статистичке податке о инцидентима у ИКТ систему.

Угрожавање ИКТ система од посебног значаја могло би да изазове последице по функционисање организација које њима управљају, али и на права и интересе грађана и привреде, као и на националну и јавну безбедност. Идентификовани проблеми са којима се суочавају ИКТ системи од посебног значаја односе се на недостатак довољног броја запослених (посебно оних са адекватим знањем), неодговарајућу опрему и недовољно развијену свест руководства о значају информационе безбедности. Ови проблеми су посебно изражени у јавном сектору. У приватном сектору постоји издвајање већих финансијских средстава за информациону безбедност.

Недостатак капацитета за реаговање на инциденте у државним институцијама

И поред обавезе предвиђене Законом о информационој безбедности, нису све институције у јавном сектору развиле капацитете за реаговање на инциденте. Органи управе имају проблем са привлачењем и задржавањем кадра за ове послове, о чему се посебно мора водити рачуна у будућности. Чак и институције које су формално успоставиле своје организационе целине и радиле на изградњи њихових капацитета морају континуирано да унапређују своје капацитете, док они који своје капацитете још увек нису изградиле могу добити, и добијају је, од стране оних који су одмакли у овом процесу.

Национални ЦЕРТ, који је основан 2017. године, и даље има потребе за подизањем капацитета, без обзира што је у претходном периоду доста учињено по питању ангажовања нових запослених, набавке опреме и опремања простора. Сарадња са ЦЕРТ-ом органа власти и ЦЕРТ-овима самосталних оператора ИКТ система је успостављена и редовна, али може бити побољшана кроз интензивнију размену знања и искустава и брзу помоћ у случају инцидената.

Ради ефикаснијег реаговања у случају озбиљнијих инцидената, посебно оних од националног значаја, потребно је успоставити одговарајуће протоколе и процедуре за сарадњу, одредити особе за контакт и организовати редовне вежбе.

ЦЕРТ органа власти је превасходно усмерен на заштиту у оквиру јединствене информационо-комуникационе мреже електронске управе. Значајан број органа јавне власти повезан је на мрежу електронске управе и од велике користи би било подизање њихових капацитета за реаговање у случају инцидента и побољшање размене информација са ЦЕРТ-ом органа власти.

Недостатак координације за откривање рањивости

Овај аспект последњих година добија све више на значају на глобалном нивоу. Многи истраживачи и стручњаци раде на откривању рањивости и њиховом отклањању пре него што их открију криминалци и злонамерни корисници. У таквим ситуацијама чешће се догађа да криминалци добију отворену могућност да угрозе одређени ИКТ систем него да организација успе да за кратко време отклони рањивост, па је успостављање модела за систематично обавештавање о рањивостима начин да се ови проблеми отклоне.

Недовољна координација међународних активности

Република Србија активно учествује у многим међународним организацијама и процесима у области информационе безбедности, како на глобалном тако и на регионалном нивоу, као и у билатералним активностима. Између осталог, Република Србија учествује у раду Отворене радне групе УН за питања информационе безбедности, имала је представника у петој Групи владиних експерата УН, активно учествује у раду Неформалне радне групе ОЕБС основане одлуком Сталног савета број 1039, спонзор је имплементације Мере ОЕБС за изградњу поверења број 9, члан је Глобалног форума за сајбер експертизу и има именоване представнике у свих пет радних група овог Форума. Институције из Републике Србије често учествују у активностима које се

реализују у оквиру међународних пројеката из области информационе безбедности, укључујући обуке, радионице, састанке и конференције.

Досадашња пракса подразумевала је ангажовање представника из неколико институција из јавног сектора у међународним организацијама и телима. Таква пракса није проблем сама по себи, али може довести до неконзистентног става различитих представника због мањка информација о позицији Србије или активностима представника у другим организацијама. Значајно би било успостављање обавезних консултација представника Србије у међународним организацијама у области информационе безбедности, узимајући у обзир надлежности Министарства спољних послова.

4) Која промена се предлаже и да ли је промена заиста неопходна и у ком обиму?

Измене Закона о информационој безбедности иницирane су пре свега због усклађивања са европском НИС 2 Директивом (енг. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 - NIS 2 Directive) усвојеној 14. децембра 2022. године, али и у делу сертификације ИКТ система са Актом о сајбер безбедности - Уредба 2019/881 (енг. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 - Cybersecurity Act*) усвојеној 17. априла 2019. године.

Поред тога, на основу досадашње примене Закона утврђене су и друге потребе које због недовољне имплементације свих законских решења захтевају не само измену правног, већ и институционалног оквира. Због тога ће посебно бити представљене најпре промене важећег институционалног оквира уређеног Законом, а затим и друге измене, као резултат хармонизације са европским правним оквиром.

Предлози измена институционалног оквира

Недостатак капацитета надлежних органа у области информационе безбедности захтева и измену институционалног оквира. У циљу проналажења најбољег модела анализирани су примери институционалног оквира три европске земље: Савезне Републике Немачке, Великог Војводства Луксембург и Краљевине Холандије који су представљени у наставку.

Савезна Република Немачка

За област информационе безбедности на федералном нивоу у Немачкој је надлежно федерално Министарство унутрашњих послова (Министарство унутрашњих послова и заједнице). Међутим, Немачка је земља са јаким федерализмом и надлежности федералних јединица су веома широке, па је регулисање области информационе безбедности представљало велики изазов за ову државу, што је чак довело и до измена Устава.

Прву стратегију информационе безбедности Немачка је усвојила 2011. године, 2016. године је усвојила измене те стратегије, а 2021. године је усвојила нову Стратегију информационе безбедности за Немачку. У новој Стратегији дефинисана су четири принципа:

- Успостављање информационе безбедности као заједничког задатка за Владу, приватни сектор, истраживачку заједницу и друштво у целини,
- Оснаживање дигиталног суверенитета Владе, приватног сектора, истраживачке заједнице и друштва у целини,

- Остваривање безбедне дигиталне трансформације и
- Постављање мерљивих и транспарентних циљева.

Надлежност пружања информационе безбедности на националном нивоу има Федерална канцеларија за информациону безбедност (Bundesamt für Sicherheit in der Informationstechnik, BSI). Ова Канцеларија успостављена је 1991. године и припада немачком федералном Министарству унутрашњих послова, а надлежности су јој додељене Актом о Федералној канцеларији за информациону безбедност који је регулисао област информационе безбедности у Немачкој на националном нивоу. Седиште Канцеларије је у Бону, а тренутно има преко 1400 запослених.

Након усвајања НИС Директиве ЕУ, у Немачкој је њихов правни систем усклађен амандманима на Акт о Федералној канцеларији за информациону безбедност и на неколико других закона у области јавних сервиса. Неке од надлежности које има БСИ како би испунила своје задатке су:

- Превенција претњи по безбедност федералних ИКТ система,
- Тестирање и процена безбедности ИКТ система и компоненти и издавање безбедносних сертификата, и
- Развој техничких безбедносних стандарда за федералне ИКТ системе.

Нове измене правног оквира направљене су 2021. године усвајањем у Бундестагу Акта о ИТ безбедности Немачке 2.0 (прва верзија усвојена је 2015. године) којима је Федерална канцеларија за информациону безбедност добила нове и ојачала постојеће надлежности у следећим областима:

- Детекција и одбрана – повећане надлежности у детекцији безбедносних рањивости и одбрани од сајбер напада, овлашћења за постављање обавезујућих минималних стандарда за федералне институције, мониторинг имплементације постављених стандарда, постављање правила за безбедну дигитализацију;
- Безбедност у мобилним мрежама – уређење забране коришћења критичних компоненти, безбедносни захтеви за операторе мобилних сервиса, обавеза сертификације критичних компоненти, примена информационе безбедности у 5G мобилним мрежама;
- Заштита потрошача – саветовања потрошача о безбедносним питањима (нова функција Канцеларије), увођење ознаке „IT Security Mark“ на производима;
- Безбедност пословања – проширење критичне инфраструктуре на област одлагања смећа, обавеза имплементације безбедносних мера за организације од посебног јавног интереса (које не припадају критичној инфраструктури);
- Национална сајбербезбедносна сертификација – надлежности Националног ауторитета за сајбербезбедносну сертификацију (у складу са Актом о сајбер безбедности ЕУ).

Организациона структура Федералне канцеларије за информациону безбедност састављена је од осам директората:

- Централни послови,
- Технички центар изврсности,
- Технологије информационих уверења и управљање ИТ,
- Оперативна информациона безбедност,
- Стандардизација, сертификација и информациона безбедност телекомуникационих мрежа,
- Информациона безбедност за дигитализацију и електронске идентитете,
- Консултације за институције Федерације, федералних јединица и локалних власти и
- Информациона безбедност за приватни сектор и друштво.

Сваки од директората организован је кроз ниже организационе јединице. Канцеларијом управља председник, којем су директно подређене још три организационе јединице:

- Биро за стратешке комуникације и медије,
- Јединица за стратешку контролу и интерне провере и

- Јединица за стратешку и извршну подршку.

У оквиру Канцеларије делују неке од најзначајнијих организационих целина за сајбер одбрану:

- Национални центар за сајбер одбрану – платформа за сарадњу и размену информација о сајбер претњама и за усклађивање активности Владе на превенцији и сузбијању сајбер напада; у раду Националног центра учествују представници полиције, служби безбедности (војних и цивилних), федералне канцеларије за цивилну заштиту и помоћ у ванредним ситуацијама и војне сајбер команде;
- Савез за информациону безбедност – јавно-приватно партнерство у области информационе безбедности у којем учествује преко 4000 компанија;
- Федерални ЦЕРТ (CERT-Bund) – централна тачка контакта за превентивне и реактивне мере у случајевима сајбер инцидената у федералним институцијама; и
- ИТ Ситуациони центар – надлежан за координацију одговора у случајевима сајбер инцидената.

Савет за информациону безбедност формиран је 2011. године на основу Стратегије за информациону безбедност Немачке и са циљем да унапреди сарадњу на нивоу федералне Владе у области информационе безбедности. Измене Стратегије из 2016. године дефинисале су перманентну улогу овог Савета као саветодавног органа федералне Владе. Састанцима Савета руководи Главни службеник за информисање (CIO) федералне Владе. Савет има обавезу да Влади подноси извештаје о стратешким питањима у области информационе безбедности о којима расправља. Од 2018. године успостављена је и посебна радна група са задатком да помаже Савету у раду.

Проблем са којим се суочавају све земље, па и Немачка, јесте прављење разлике између унутрашње безбедности, која је традиционално у надлежности полиције, и спољне безбедности, која је традиционално у надлежности војске. У сајбер простору ова граница није сасвим јасна, а све већа употреба сајбер простора за војне активности намеће потребу да се одређене активности дефинишу и спроведу. Из тог разлога Немачка је 2017. године дефинисала сајбер и информациони војни домен, поред постојећих копненог, поморског и ваздушног, и успоставила нову службу надлежну за овај домен. Према расположивим подацима у овој служби је 2020. године било запослено преко 14.000 цивилног и војног особља. Такође, из разлога специфичности сајбер простора по питању унутрашње и спољне безбедности, договором немачких политичких партија је 2018. године одлучено да се формира заједничка агенција Министарства одбране и Министарства унутрашњих послова са задатком да спроводи креативне и иновативне пројекте из области информационе безбедности. На основу овог договора, 2020. године формирана је Сајбер агенција (Agentur für Innovation in der Cybersicherheit или Cyberagentur) у форми компаније са ограниченом одговорношћу (GmbH) чији је једини акционар федерална Влада. Ова Агенција има око 100 запослених (према расположивим подацима) и не спроводи самостално истраживања, већ у сарадњи са академијом и индустријом спроводи иновативне пројекте за које се процени да су од изузетног националног значаја (посебно их интересују теме као што су поуздане и отпорне информационе технологије, интеракција човека и технологије, вештачка интелигенција, нано и квантна технологија, свемирска и поморска безбедност, бионика, интерфејси мозак-рачунар, предиктивна аналитика, криптографија или аутономни системи). Агенција је за своје активности добила иницијални буџет од 280 милиона евра од којих је већи део већ уложила у истраживачке пројекте.

Још једна значајна платформа коју је покренуло немачко Министарство одбране је Сајбер иновациони хаб, са намером да привуче младе и креативне умове да кроз стартап-ове и окружење које више одговара њиховом начину размишљања реализују пројекте од значаја за одбрану.

Сајбер иновациони хаб је у суштини платформа за реализацију пројеката, а формално је организован као огранак компаније која пружа ИТ услуге за немачку армију, која доноси крајњу одлуку који пројекти ће се финансирати.

Велико Војводство Луксембург

Документ јавних политика у области информационе безбедности у Луксембургу је национална стратегија информационе безбедности. До сада је Луксембург усвојио четири стратегије, а последња се односи на период од 2021. до 2025. године. Свака од стратегија доносила је одређена унапређења, па је тако прва стратегија иницирала оснивање Владиног ЦЕРТ-а, друга успостављање Националне агенције за безбедност информационих система (фра. *Agence nationale de la sécurité des systèmes d'information - ANSSI*), трећа формирање Центра за компетенције у области информационе безбедности (енг. *Cybersecurity Competence Center - C3*), успостављање методологије за анализу ризика *MONARC* и формирање Међуминистарског координационог комитета за сајбер превенцију и информациону безбедност (Comité interministériel de coordination en matière de cyberprévention et de cybersécurité), док четврта предвиђа формирање *SOC* за критичну инфраструктуру, формирање Националног центра за филтрирање *DDoS* напада, развој платформе за анализу и управљање ризицима *SERIMA* намењене операторима есенцијалних сервиса и друго. Институција надлежна за израду и координацију стратегије је Високи комесаријат за националну заштиту (HCPN).

Луксембург је у мају 2019. године транспоновао НИС Директиву ЕУ у своје законодавство и одредио Регулаторни институт Луксембурга *ILR* за јединствену тачку контакта и надлежни орган за секторе енергетике, транспорта, здравља, пијаће воде и дигиталне инфраструктуре, док је Комисија за надзор сектора финансија *CSSF* надлежни орган за секторе инфраструктуре финансијских тржишта и кредитних институција.

Луксембург нема централни орган који би обједињавао надлежности у области информационе безбедности, него су надлежности дате различитим институцијама. Стратешке надлежности имају две институције: Тело за информациону безбедност *CSB* и Међуминистарски координациони комитет за сајбер превенцију и информациону безбедност (CIC-CPCS). Надлежност над координацијом активности ова два тела и задатак стратешког вођства има Високи комесаријат за националну заштиту.

Тело за информациону безбедност формирано је 2011. године са задатком да имплементира и надзире извршавање прве националне стратегије, а од 2019. године налази се у надлежности Министарства државе.

Међуминистарски координациони комитет за сајбер превенцију и информациону безбедност успостављен је 2017. године са циљем да се, у сарадњи са Телом за информациону безбедност, ангажује на координацији оперативних активности. У раду Комитета учествују представници следећих институција:

- Министарство државе,
- Високи комесаријат за националну заштиту,
- Одбрана Луксембурга (Директорат за одбрану и Оружане снаге Луксембурга),
- Министарство привреде,
- економска интересна група SECURITYMADEIN.LU,
- Владин центар за информационе технологије (CTIE),
- Државна обавештајна служба,
- Национална агенција за безбедност информационих система (ANSSI) и

- Владин ЦЕРТ (GovCERT).

Радом комитета председава Високи комесар за националну заштиту. Задаци који су постављени пред овај Комитет су:

- обезбеђење конзистентности акција и иницијатива,
- координација имплементације иницијатива које долазе од ЕУ или са других међународних нивоа,
- надзор над имплементацијом ових иницијатива,
- давање савета Влади по питањима информационе безбедности и
- дискусија о ставовима националних представника.

Високи комесаријат за националну заштиту је тело које је постојало током Хладног рата као канцеларија Комитета за националну заштиту (са задацима везаним за заштиту органа власти и становништва, прикупљање обавештајних података, спровођење психолошких операција и слично) и потом укинуто, али је реактивирано након терористичких напада 11. септембра 2001. са новим надлежностима у области заштите критичне инфраструктуре и од 2016. године уврштено у састав Министарства државе. Високи комесаријат је надлежан за превенцију и управљање сајбер кризама и за планирање одговора на ванредне ситуације у области информационе безбедности. За сајбер дипломатију надлежно је Министарство спољних и европских послова.

Национална агенција за безбедност информационих система (ANSSI) је надлежна за системе у државним органима. Ова Агенција је формирана 2015. године и саставни је део Високог комесаријата за националну заштиту као регулаторни орган. Неке од надлежности ANSSI су:

- израда политика и водича за заштиту класификованих и некласификованих информација,
- обезбеђење примене мера заштите информационих система,
- сертификација начина обраде некласификованих информација,
- функције Националног и Владиног ЦЕРТ-а и
- надлежни орган за ТЕМПЕСТ.

ANSSI је до 2018. године био и надлежни орган за одобравање криптографских производа, када су те надлежности пренете на Владин центар за информационе технологије (CTIE). ANSSI је до те године био и тело надлежно за управљање сајбер инцидентима, када је та улога пренета на Владин ЦЕРТ. Владин центар за информационе технологије (CTIE) је основан 2009. године и представља централни орган за послове везане за информационе технологије за министарства и државну администрацију. CTIE је такође и надлежни орган за дистрибуцију криптографског материјала и надлежни орган за криптографску акредитацију, а у надлежности му спадају и заштићена комуникација и размена информација између државних органа.

Владин ЦЕРТ (GovCERT) је основан 2013. године са задатком да решава све озбиљније сајбер инциденте у ИКТ системима Владе. Од 2015. године GovCERT је од ANSSI преузео надлежности управљања сајбер инцидентима и објединио улоге Националног и Владиног ЦЕРТ-а, а од 2018. године му је, поред постојећих, поверена и функција Војног ЦЕРТ-а (MilCERT) и смештен је у Високи комесаријат за националну заштиту. У оквиру надлежности Националног ЦЕРТ-а, GovCERT је званична национална тачка контакта са ЦЕРТ-овима других земаља и тачка за контакт и размену информација са секторским ЦЕРТ-овима у Луксембургу. GovCERT, у оквиру својих надлежности као Војни ЦЕРТ, делује као званична тачка контакта за војне ЦЕРТ-ове других земаља, али и прати и реагује на инциденте у ИКТ системима Оружаних снага.

Економска интересна група Security Made in Lëtzebuerg (познатија као SECURITYMADEIN.LU) је основана 2010. године са мандатом од Министарства привреде (које и надзире њен рад) да

спроводи истраживања на међународном нивоу, дели информације о претњама, имплементира мрежу сензора за рана упозорења и делује као хаб за економске активности у овој области. Финансијска средства за рад групе обезбеђује држава. SECURITYMADEIN.LU у свом саставу има три организационе јединице: Центар за реаговање на компјутерске инциденте (енг. *Computer Incident Response Center Luxembourg - CIRCL*), Сервисе подизања безбедносне свести у сајбер свету и безбедносна побољшања (CASES) и Центар за компетенције у области информационе безбедности (C3).

Можда и најпознатија организација из области информационе безбедности из Луксембурга је CIRCL који је надлежан за приватни сектор, локалну самоуправу и невладине организације. CIRCL је глобално познат по својој платформи за дељење информација о претњама MISP, а од других иницијатива у којима учествује вреди поменути заједницу CERT.LU која обезбеђује размену информација и сарадњу приватних ЦЕРТ-ова са CIRCL и GovCERT.

Cyberworld Awareness and Security Enhancement Services Luxembourg (CASES) обезбеђује публикације, едукативни материјал, примере најбољих пракси и разне алате везане за информациону безбедност (између осталог, метод за анализу ризика MONARC).

Центар за компетенције у области информационе безбедности (C3) активности реализује кроз давање мишљења, тренирање и тестирање, претежно за приватни сектор.

Национални ауторитет за сертификацију у области информационе безбедности је Институт за стандардизацију, акредитацију, сигурност и квалитет производа и услуга (ILNES).

Луксембург има усвојен план за реаговање у случају сајбер кризе (фра. *Plan d'intervention d'urgence en cas d'attaque contre les systèmes d'information ou de faille technique des systèmes d'information - PIU Cyber*) за чију рализацију је одговоран директно премијер. Овај план је развијен од стране Високог комесаријата за националну заштиту и има четири главна циља:

- усвајање заштитних и превентивних мера,
- дефинисање улоге ентитета за управљање кризама,
- дефинисање мера, поступака и актера у случајевима ванредних ситуација и
- узбуњивање и информисање јавности.

План предвиђа успостављање четири *ad-hoc* јединице за решавање кризе: јединице за кризу, оперативне јединице, јединице за процену сајбер ризика и јединице за комуникације и информисање. План укључује задатке сваке од ових јединица, њихов састав, субординацију, извештавање и све остале елементе који су потребни за успешно решавање кризе.

<u>Краљевина Холандија</u>

Холандија је прву стратегију информационе безбедности усвојила 2011. године, а тренутно важећа је стратегија усвојена за период од 2022. до 2028. године. Нова Стратегија усмерава активности у четири главна смера:

- побољшање друштвене отпорности кроз заједничке напоре јавног, приватног и невладиног сектора,
- подстицање безбедности дигиталних производа и услуга у складу са прописима ЕУ,
- сузбијање сајбер претњи које потичу од држава и криминалаца кроз побољшање прикупљања и дељења информација, и у јавном и приватном сектору и
- обезбеђење квалитетне радне снаге у области информационе безбедности, образовање и подизање свести грађана.

Једна од најважнијих активности планирана Стратегијом је спајање неколико организација са преклапајућим надлежностима - NCSC, Центра за дигитално поверење (DTC) и ЦСИРТ-а провајдера дигиталних сервиса (CSIRT-DSP) у једну организацију, која ће постати јединствени национални ауторитет за информациону безбедност. Холандија је овом Стратегијом исказала снажну посвећеност обједињавању постојећих капацитета и неопходност брзе спознаје информација о претњама и рањивостима и реаговања на ове информације. Стратегијом је чак наглашена потреба сузбијања фрагментације у дељењу информација кад год је могуће и потреба за рестриктивношћу у формирању нових ЦЕРТ-ова. У том циљу, нови ауторитет (за који се очекује да ће бити успостављен током 2024. године) радиће у сарадњи са јавним и приватним сектором и пружати информације о безбедности свим секторима, организацијама које спадају и које не спадају у критичну инфраструктуру и генералној јавности.

У Холандији је препознато више од 20 институција са индивидуалном и колективном одговорношћу у области информационе безбедности. На политичком и стратешком нивоу најважније тело је Савет за информациону безбедност.

Савет за информациону безбедност формиран је 2011. године као тело које треба да повеже различите актере из јавног и приватног сектора и са мандатом да саветује Владу и приватни сектор, постави националне приоритете, процени потребе за истраживањем и развојем и обезбеди размену знања у оквиру јавног и приватног сектора. За рад Савета надлежно је Министарство безбедности и правде, а у раду Савета учествују представници из јавног и приватног сектора. Јавни сектор је заступљен са 15 представника из следећих институција:

- Национални координатор за безбедност и сузбијање тероризма (у саставу Министарства безбедности и правде),
- Министарство економских послова,
- Министарство одбране,
- Генерални обавештајни и безбедносни сервис,
- Агенција за националне полицијске сервисе и
- Генерални одбор тужилаца.

Из приватног сектора у раду Савета учествују представници водећих провајдера телекомуникационих услуга, водећих снабдевача ИКТ опремом, корисника ИТ услуга, малих и средњих предузећа, оператора критичне инфраструктуре и академских институција. Радом Савета копредседавају Национални координатор за безбедност и сузбијање тероризма и представник приватног сектора (који се периодично мења).

Национални центар за информациону безбедност (NCSC) формиран је 2012. године са задатком да унапреди разумевање развоја, претњи и трендова у области информационе безбедности и преузме одговорност у решавању сајбер инцидената и управљању сајбер кризама. У састав NCSC приликом оснивања инкорпориран је постојећи Владин ЦЕРТ (GOVCERT.NL). У надлежност NCSC спада пружање услуга Влади и ИКТ системима критичне инфраструктуре у јавном и приватном сектору, као и унапређење јавно-приватног партнерства. NCSC је организационо смештен у Директорату за информациону безбедност Министарства безбедности и правде, а директно је потчињен Националном координатору за безбедност и сузбијање тероризма. NCSC чине три тима са надлежностима за реаговање на инциденте, едукацију и развој. У Директорату за информациону безбедност постоји и посебно Одељење за политике у чијој је надлежности развој политика и стратегија у области информационе безбедности.

Надлежност NCSC обухвата поступање са претњама и инцидентима, подизање безбедносне свести, давање савета, реаговање у случају кризе и пружање платформе за сарадњу. NCSC је

такође веома активан у међународној сарадњи и национална тачка контакта Холандије. NCSC има кључну координациону улогу у случају озбиљног сајбер инцидента или сајбер кризе. Да би успешно остварио овај задатак, NCSC континуално прати стање, врши процене угрожености и могућих последица и реагује у случају потребе. Једна од најважнијих активности NCSC је управо прикупљање информација, како од јавног и приватног сектора у Холандији тако и од међународних партнера.

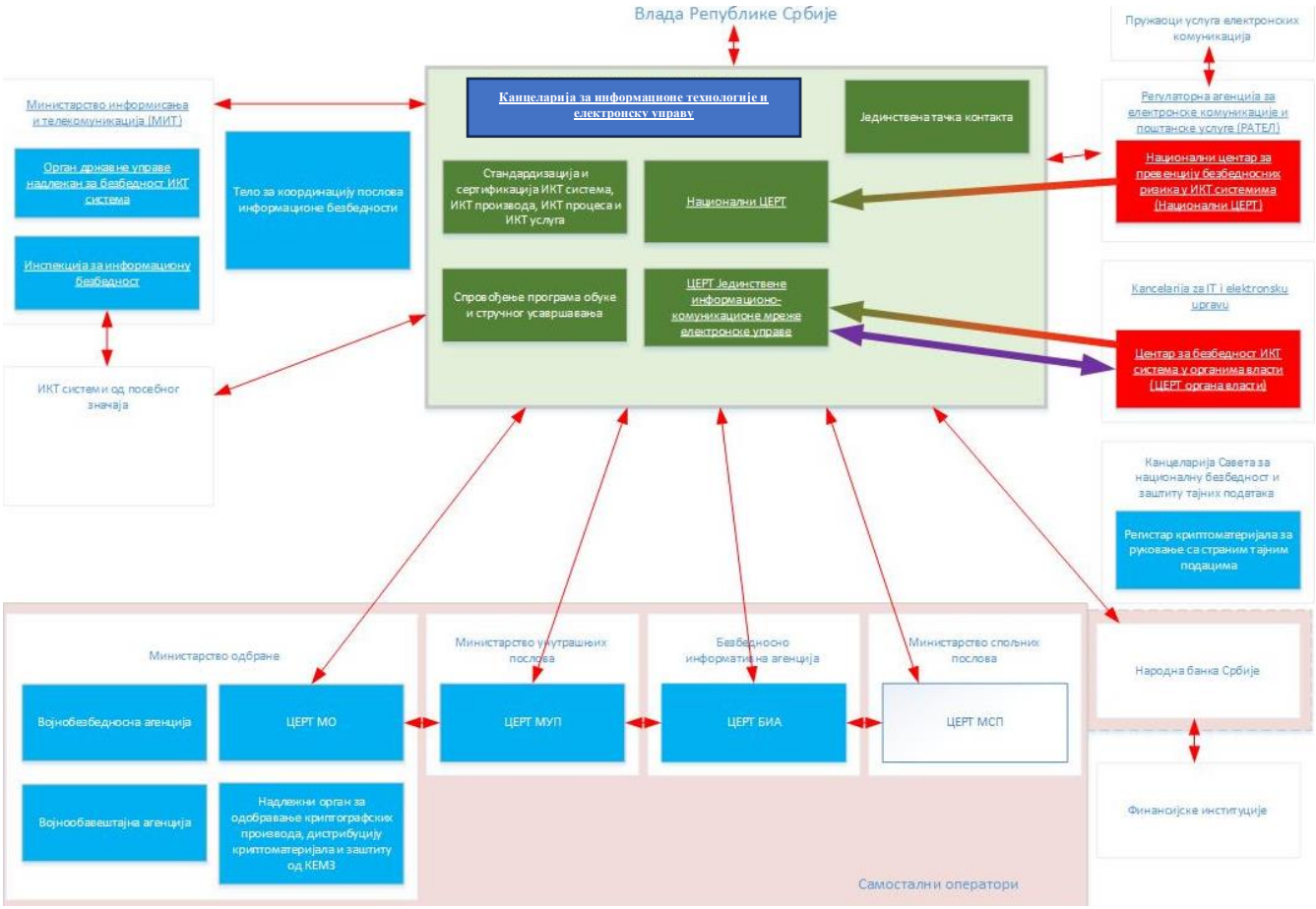
У случају озбиљног сајбер инцидента или сајбер кризе NCSC активира Одбор за ИКТ одговор (IRB) и даје подршку његовим активностима кроз прибављање и дистрибуцију информација и административну подршку. С обзиром да је у Холандији велики део критичне инфраструктуре у приватном сектору, у раду IRB учествују, поред представника институција Владе, и представници провајдера телекомуникационих услуга, енергетског и финансијског сектора, а по потреби се могу укључити и други експерти. Радом IRB руководи представник Министарства економских послова. Примарни задатак IRB је да саветује национална тела за управљање кризама о мерама које треба предузети, али такође и да служи као тело које у случају кризе спаја технички и административни ниво.

Холандија је 2012. године препознала сајбер простор као пети домен војних операција (поред земље, мора, ваздуха и свемира) и дефинисала шест области развоја сајбер капацитета: одбрана, напад, обавештајне активности, адаптивност, иновације и сарадња. Заједничка команда за управљање информацијама (JIVC) формирана је 2013. године, а у њен састав ушао је и ЦЕРТ одбране (DefCERT) формиран годину дана раније. Надлежности DefCERT су у домену безбедности ИКТ система Министарства одбране и Оружаних снага Холандије, подршке војним операцијама, процене претњи и рањивости, давања савета и слично, али такође и подршка државним органима у заједничком одговору на сајбер претње. DefCERT и NCSC су потписали меморандум о разумевању и интензивно сарађују кроз размену информација и узајамну подршку.

Одбрамбена сајбер команда је формирана 2014. године са примарним фокусом на успостављање одбрамбених, нападачких и обавештајних капацитета у сајбер простору. У састав Одбрамбене сајбер команде приликом успостављања ушле су организационе јединице осталих служби, чиме је успостављена јединствена целина у одбрамбеном систему Холандије надлежна за ову област.

Предлози унапређења институционалног оквира у Републици Србији

Анализа постојећег институционалног оквира указује на расипање капацитета надлежних органа за превентивно и благовремено реаговање на инциденте у сајбер простору. Уместо оснивања новог органа, Република Србија је одлучила да одређене надлежности у области информационе безбедности пренесе на Канцеларију за информационе технологије и електронску управу. Овакво решење омогућава бољу искоришћеност постојећих ресурса и јачање капацитета, без потребе за додатним институционалним променама. У складу са наведеним моделима европских земаља, анализирана су три модела институционалне промене који су дати у наставку.



Дијаграм 19 Институционални оквир - модел 1

Новина:

- Канцеларија за информационе технологије и електронску управу постаје јединствена тачка контакта у области информационе безбедности.
- На Канцеларију за информационе технологије и електронску управу преносе се надлежности Националног ЦЕРТ-а и Владиног ЦЕРТ-а, укључујући постојеће организационе јединице и запослене.

Предности оваквог модела институционалног оквира су:

- Успостављање јединствене, препознатљиве институције у оквиру постојећег система државне управе.
- Груписање постојећих капацитета, што омогућава бољу и бржу размену информација.
- Обезбеђивање услова за конкретну помоћ другим органима државне управе у случају сајбер инцидената, укључујући подршку малим и средњим предузећима (МСП) и другим субјектима.

Недостаци оваквог модела институционалног оквира су:

- Потреба за додатним улагањем у јачање капацитета Канцеларије за информационе технологије и електронску управу како би се ефикасно одговорило на све захтеве јавног сектора.

Другим моделом:

- Канцеларија за информационе технологије и електронску управу постаје Надлежни орган и јединствена тачка контакта у области информационе безбедности.

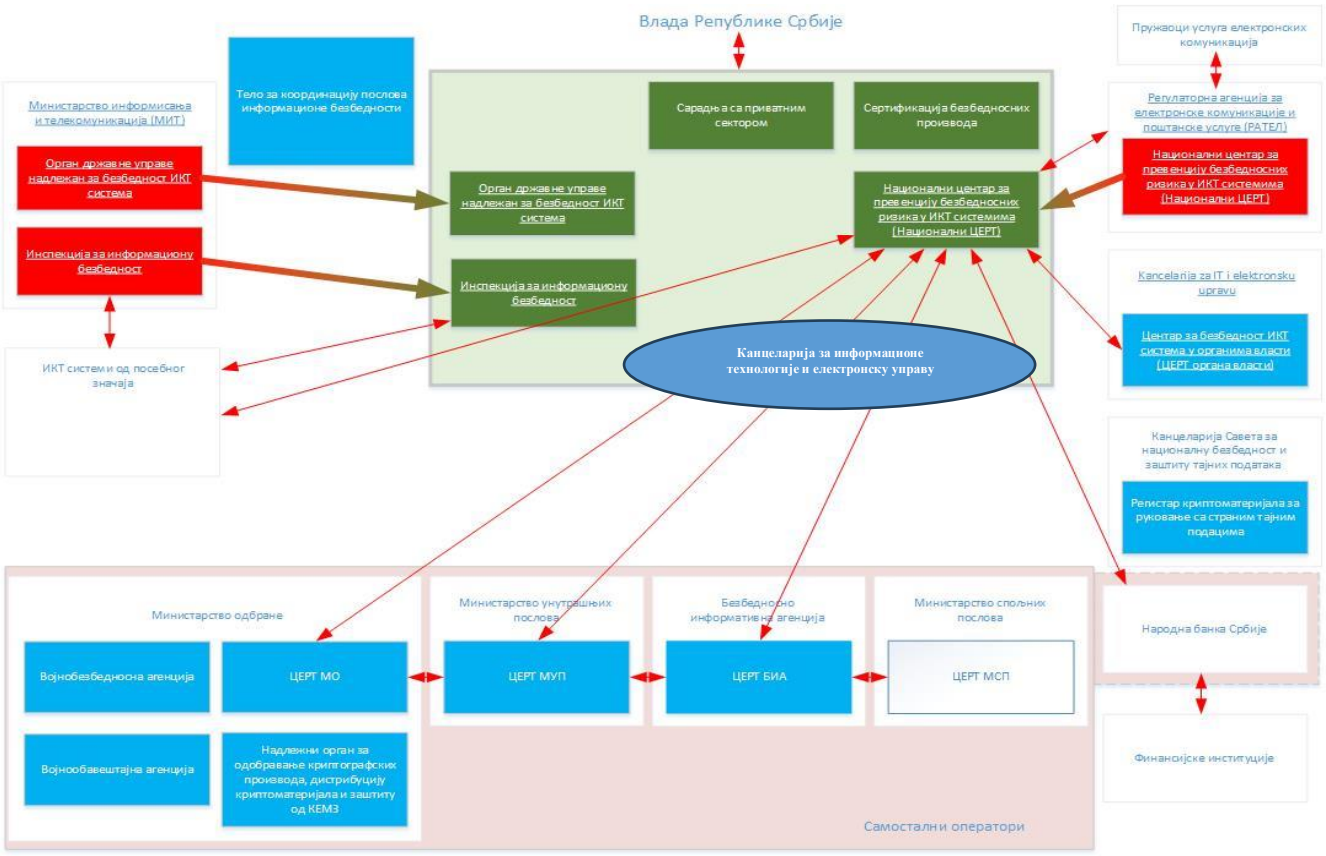
- На Канцеларију за информационе технологије и електронску управу преносе се надлежности Инспекције за информациону безбедност и Националног ЦЕРТ-а, укључујући постојеће организационе јединице и запослене.

Предности оваквог модела институционалног оквира су:

- Повећање капацитета за подршку ИКТ системима од посебног значаја.
- Обезбеђивање услова за бољу и бржу размену информација између релевантних субјеката.

Недостаци оваквог модела институционалног оквира су:

- Ограничене могућности за сарадњу по питању оперативних активности уколико се капацитети недовољно унапреде.
- Изазови у прихватању преноса надлежности и интеграције запослених у оквиру постојеће институције.



Дијаграм 20 Институционални оквир - модел 2

Трећим моделом:

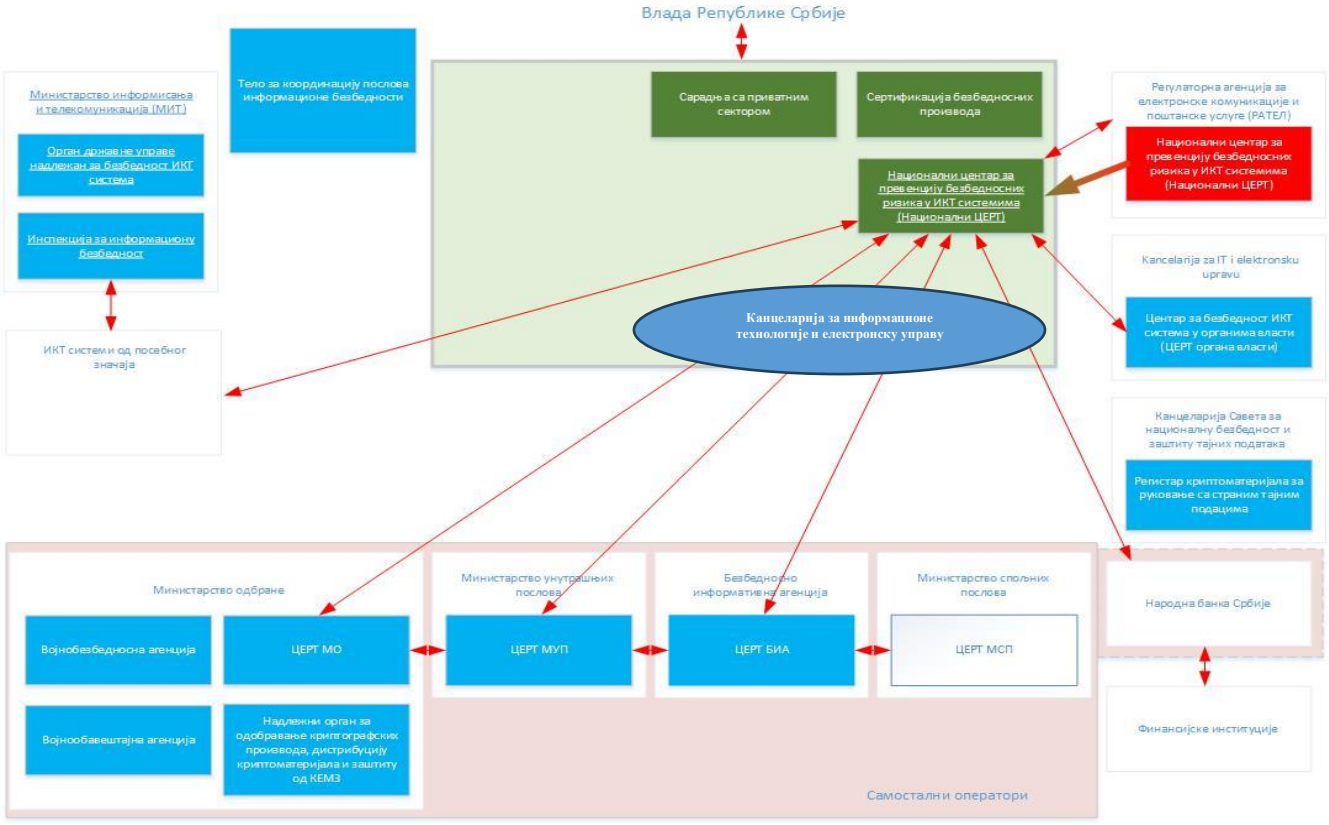
- Надлежности Националног ЦЕРТ-а преносе се на Канцеларију за информационе технологије и електронску управу.

Предности оваквог модела институционалног оквира су:

- Бржа имплементација модела, јер не захтева оснивање нове организације нити велике структурне промене.

Недостаци оваквог модела институционалног оквира су:

- Потреба за додатним улагањем у капацитете Канцеларије за информационе технологије и електронску управу како би могла у потпуности да одговори на нове захтеве у области информационе безбедности.



Дијаграм 21 Институционални оквир - модел 3

Након анализе модела и пракси европских земаља одлучено је да се прихвати **први модел.**

Након анализе модела и пракси европских земаља, одлучено је да се надлежности у области информационе безбедности пренесу на постојећу Канцеларију за информационе технологије и електронску управу.

Према члану 28. Нацрта закона, Канцеларија обавља следеће послове:

- *Превенција и заштита од безбедносних ризика на националном нивоу (послови Националног ЦЕРТ-а);*
- *Предузимање мера за заштиту Јединствене информационо-комуникационе мреже (послови ЦЕРТ-а органа власти);*

- *Вршење послова јединствене тачке контакта;*
- *Сарадња на националном и међународном нивоу у области информационе безбедности;*
- *Сертификација ИКТ система, производа, процеса и услуга изузев система, производа, процеса и услуга за потребе одбране и безбедности и ИКТ система за рад са тајним подацима;*
- *Прописивање минималних мера заштите ИКТ система органа;*
- *Стручни надзор над радом оператора ИКТ система од посебног значаја;*
- *Вођење базе рањивости ИКТ производа и услуга;*
- *Развој обука и стручног усавршавања;*
- *Квартално извештавање Министарства;*
- *Обављање других послова у складу са законом.*

Овај модел омогућава ефикаснију употребу постојећих ресурса и јачање капацитета Канцеларије за информационе технологије и електронску управу, без потребе за формирањем нове организације.

Канцеларија за информационе технологије и електронску управу послове из своје надлежности прописане овим законом почиње да обавља даном истека периода од 12 месеци од дана ступања на снагу овог закона.

Регулаторно тело за електронске комуникације и поштанске услуге обавља послове Националног ЦЕРТ-а утврђене овим законом до истека периода од 12 месеци од дана ступања на снагу овог закона.

Министарство и даље води евиденцију оператора ИКТ система од посебног значаја и врши надзор над радом Канцеларије за информационе технологије и електронску управу.

На овај начин удружују се постојећи капацитети два ЦЕРТ-а, што би у значајној мери требало да побољша координацију и реаговање на инциденте.

Усклађивање са европским прописима

Директива ЕУ 2022/2555 о мерама за висок заједнички ниво информационе безбедности широм Уније утврђује мере које имају за циљ постизање високог заједничког нивоа информационе безбедности унутар ЕУ како би се побољшало функционисање унутрашњег тржишта. Овом Директивом дати су амандмани на Уредбу ЕУ 910/2014 о електронској идентификацији и услугама од поверења (eIDAS) и на Директиву ЕУ 2018/1972 о кодексу електронских комуникација.

Директивом се:

- утврђује обавеза за све државе чланице да усвоје националну стратегију о безбедности мрежних и информационих система, да именују националне надлежне органе (компетентне ауторитете), органе надлежне за управљање сајбер кризама, јединствене тачке контакта и ЦСИРТ-ове;
- утврђују обавезе по питањима мера за управљање ризиком и извештавање за ентитете одређене као есенцијалне или важне у складу са овом Директивом, као и за ентитете идентификоване као критичне у складу са Директивом ЕУ 2022/2557 (CER Директива);
- утврђују правила и обавезе у вези дељења информација; и

- утврђују обавезе држава чланица ЕУ по питањима примене ове Директиве и надзора над применом.

  Нацртом закона о информационој безбедности (у даљем тексту: Нацрт закона):
  - *уређују се мере заштите од безбедносних ризика у информационо-комуникационим системима;*
  - *уређују се одговорности правних лица приликом управљања и коришћења информационо-комуникационих система;*
  - *уређују се поступци и мере за постизање високог општег нивоа информационе безбедности; и*
  - *одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите, као за надзор над спровођењем овог закона*.

Директива НИС 2 је применљива на ентитете који се сматрају предузећима најмање средње величине и који своје делатности обављају унутар Европске Уније у секторима који су одређени као високо критични или критични. Поред тога, ова Директива примењује се и на ентитете, без обзира на њихову величину, који су идентификовани као критични у складу са Директивом 2022/2557 или који пружају услуге регистрације имена домена, као и на све друге ентитете из високо критичних или критичних сектора, без обзира на њихову величину:

- који пружају услуге јавних електронских комуникационих мрежа, услуге од поверења, услуге регистрације домена највишег нивоа или услуге ДНС;
- који су једини пружаоци неке есенцијалне услуге у држави чланици;
- чији би прекид у пружању услуга могао имати значајан утицај на јавну сигурност, јавну безбедност и јавно здравље;
- чији би прекид у пружању услуга могао имати значајан системски ризик;
- који су критични због специфичне важности на националном или регионалном нивоу;
- који спадају у државне органе на централном нивоу, или спадају у државне органе на регионалном нивоу ако би прекид пружања њихових услуга имао значајан утицај на критичне друштвене или економске активности.

Ова Директива не примењује се на државне органе надлежне за националну безбедност, јавну безбедност, одбрану и спровођење закона. Директивом су дефинисане две категорије ентитета: есенцијални и важни.

Есенцијалним ентитетима сматрају се:

- ентитети који превазилазе величину средњих предузећа (имају више од 250 запослених и обрт од преко 50 милиона евра) и који своју делатност обављају у неком од високо критичних сектора;
- пружаоци квалификованих услуга од поверења, пружаоци услуге регистрације домена највишег нивоа и пружаоци услуга ДНС без обзира на величину;
- пружаоци услуга јавних електронских комуникационих мрежа или јавно доступних електронских комуникационих услуга који спадају у предузећа средње величине;
- органи државне управе на централном нивоу;
- сви други ентитети који своје делатности обављају у високо критичним или критичним секторима, а које је држава чланица идентификовала као есенцијалне јер су једини пружаоци неке есенцијалне услуге, јер би прекид у пружању услуга могао имати значајан утицај на јавну сигурност, јавну безбедност и јавно здравље, јер би прекид у пружању услуга могао имати значајан системски ризик, или који су критични због специфичне важности на националном или регионалном нивоу;

- ентитети идентификовани као критични у складу са Директивом 2022/2557;
- сви други ентитети идентификовани као есенцијални у складу са Директивом 2016/1148 (НИС Директива), ако држава чланица процени да је то потребно.

Важним ентитетима сматрају се ентитети који своје делатности обављају у високо критичним или критичним секторима, а који не испуњавају критеријуме да буду идентификовани као есенцијални. Такође, важним ентитетима се сматрају и они које је држава чланица идентификовала као важне јер су једини пружаоци неке есенцијалне услуге, јер би прекид у пружању услуга могао имати значајан утицај на јавну сигурност, јавну безбедност и јавно здравље, јер би прекид у пружању услуга могао имати значајан системски ризик, или који су критични због специфичне важности на националном или регионалном нивоу. У секторе високе критичности спадају:

- енергетика,
- саобраћај,
- банкарство,
- инфраструктуре финансијских тржишта,
- здравље,
- пијаћа вода,
- отпадне воде,
- дигитална инфраструктура,
- управљање ИКТ услугама,
- јавна администрација и
- свемир.

У остале критичне секторе спадају:

- поштанске и курирске услуге,
- управљање отпадом,
- производња и снабдевање хемикалијама,
- производња, обрада и дистрибуција хране,
- друге производне делатности (производња медицинских уређаја и *in vitro* дијагностичких медицинских средстава, рачунара, електронских и оптичких производа, електричне опреме, машина и уређаја, моторних возила, приколица и полуприколица и производња остале опреме за превоз),
- пружање дигиталних услуга и
- истраживање.

Нацртом закона дефинисани су оператори приоритетних ИКТ система од посебног значаја који су пандан есенцијалним ентитетима, и оператори важних ИКТ система од посебног значаја који су пандан важним ентитетима из НИС 2 Директиве. Чланом 5. Нацрта закона прописано је да су оператори приоритетних ИКТ система од посебног значаја:

- *органи;*
- *субјекти који су одређени као оператори критичне инфраструктуре у складу са прописима којима се уређује критична инфраструктура;*
- *правна лица и физичка лица у својству регистрованог субјекта, која обављају послове и делатности у следећим областима:*
  - *енергетика,*
  - *саобраћај,*
  - *банкарство и финансијска тржишта,*
  - *здравство,*

- *вода за пиће ,*
- *отпадне воде ,*
- *дигитална инфраструктура,*
- *управљање ИКТ услугама које се пружају операторима приоритетних ИКТ система од посебног значаја,*
- *остале области (управљање нуклеарним објектима, пружање квалификованих услуга од поверења, пружање услуга ДНС-а, управљање регистром домена највишег нивоа са изузетком оператора коренских сервера имена, обављање делатности електронских комуникација, тачка за размену интернет саобраћаја, издавање Службеног гласника Републике Србије и вођење Правно-информационог система Републике Србије, области у којој у Републици Србији постоји само један пружалац услуге и која је неопходна за обављање критичних друштвених и привредних делатности).*

Чланом 6. Нацрта закона прописано је да су оператори важних ИКТ система од посебног значаја:

- *научноистраживачке институције;*
- *правна и физичка лица у својству регистрованог субјекта и органи који не спадају у операторе приоритетних ИКТ система од посебног значаја према критеријумима за одређивање оператора;*
- *правна лица која су дефинисана као оператори ИКТ система од посебног значаја у складу са постојећим Законом о информационој безбедности;*
- *правна лица и физичка лица у својству регистрованог субјекта, која обављају послове и делатности у следећим областима:*
  - *поштанске услуге;*
  - *управљање отпадом и амбалажним отпадом;*
  - *производња и снабдевање хемикалијама;*
  - *производња, обрада и дистрибуција хране;*
  - *производња рачунара, електронских и оптичких производа;*
  - *производња електричне опреме;*
  - *производња машина и уређаја;*
  - *производња моторних возила, приколица и полуприколица и производња остале опреме за превоз;*
  - *производња медицинских уређаја и производња in vitro дијагностичких медицинских средстава;*
  - *услуге информационог друштва у смислу закона о електронској трговини;*
  - *производња, промет и превоз наоружања и војне опреме.*

Евиденцију приоритетних и важних ИКТ система од посебног значаја успоставља и води министарство надлежно за послове информационе безбедности.

НИС 2 Директива даје дефиниције 41 термина.

У Нацрту закона дато је објашњење 57 термина, од којих 33 (идентично или у истом смислу) постоје и у НИС 2 Директиви. Термини из Нацрта закона који имају свој пандан у НИС 2 Директиви су:

- *информационо-комуникациони систем*
- *оператор ИКТ система*

- *информациона безбедност*
- *ризик*
- *рањивост*
- *избегнути инцидент*
- *претња*
- *озбиљна претња*
- *инцидент*
- *управљање инцидентом*
- *криза информационе безбедности*
- *орган*
- *услуга информационог друштва*
- *пружалац услуге информационог друштва*
- *тачка за размену интернет саобраћаја*
- *систем назива домена (ДНС)*
- *пружалац услуге ДНС-а*
- *услуга од поверења*
- *пружалац услуге од поверења*
- *квалификована услуга од поверења*
- *пружалац квалификоване услуге од поверења*
- *услуге рачунарства у клауду*
- *услуга центра за управљање и чување података*
- *научноистраживачка организација*
- *јавна електронска комуникациона мрежа*
- *електронска комуникациона услуга*
- *пружалац управљаних услуга*
- *пружалац управљаних безбедносних услуга*
- *регистар назива домена највишег нивоа*
- *пружалац услуге регистрације назива домена*
- *ИКТ производ*
- *ИКТ услуга*
- *ИКТ процес*

Термини који су дефинисани у Нацрту закона, а нису у НИС 2 Директиви су:

- *тајност*
- *интегритет*
- *расположивост*
- *аутентичност*
- *поверљивост*
- *непорецивост*
- *управљање ризиком*
- *јединствени систем за пријем обавештења о инцидентима*
- *мере заштите ИКТ система*
- *тајни податак*
- *ИКТ систем за рад са тајним подацима*
- *служба безбедности*
- *самостални оператори ИКТ система*
- *ЦЕРТ*
- *компромитујуће електромагнетно зрачење (КЕМЗ)*

- *криптобезбедност*
- *криптозаштита*
- *криптографски производ*
- *криптоматеријали*
- *безбедносна зона*
- *информациона добра*
- *TLP (Traffic Light Protocol)*
- *администратор*
- *подаци о личности*

Посебно је занимљиво дефинисање два централна термина ова два документа: информационе безбедности и сајбер безбедности. У Нацрту закона термин „информациона безбедност" има дефиницију идентичну дефиницији термина „безбедност мрежних и информационих система (security of network and information systems)" у НИС 2 Директиви, али у Нацрту закона (нити у било којем другом правном документу у Србији) не постоји дефиниција сајбер безбедности, а такође ни у НИС 2 Директиви не постоји дефиниција информационе безбедности. Мада није експлицитно дефинисан ни у НИС 2 Директиви (ни у претходној НИС Директиви) ни у Акту о сајбер безбедности, под термином „информациона безбедност" у Европској Унији се подразумева очување поверљивости, интегритета и расположивости, у складу са дефиницијом из прегледа сајбер безбедности и сродних термина који је објавила ЕНИСА[6] и дефиницијом из стандарда ИСО 27000[7].

Дефиниција термина „сајбер безбедност" је у НИС 2 Директиви референцирана на дефиницију из Акта о сајбер безбедности (Уредба ЕУ 2019/881), према којој „сајбер безбедност означава активности неопходне за заштиту мрежних и информационих система, корисника тих система и других особа на које утичу сајбер претње". Ова дефиниција може у одређеној мери да се упореди са дефиницијом термина „мере заштите ИКТ система" из Нацрта закона, према којој су то „техничке, организационе, административне и физичке мере за управљање безбедносним ризицима ИКТ система". Ипак, за ове две дефиниције не може се тврдити да имају исти смисао, па су зато у претходном набрајању сврстане у групе термина чије дефиниције немају свој пандан у другом акту.

НИС 2 Директива налаже државама чланицама да усвоје националну стратегију информационе безбедности и даје оквир тема које требају бити обухваћене стратегијом.

Нацртом закона нису прописане одредбе у вези стратегије, али је Закон препознат у Стратегији развоја информационог друштва и информационе безбедности за период 2021-2026. године.

НИС 2 Директивом је прописано да државе чланице морају одредити један или више надлежних органа (са надлежностима у одређеним секторима којима припадају оператори есенцијалних сервиса), као и јединствену тачку контакта за комуникацију са надлежним органима других

[6] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

[7] https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

земаља чланица и учешће у Групи за сарадњу. Ако је националним законодавством дефинисан само један надлежни орган, онда је тај орган истовремено и јединствена тачка контакта.

Чланом 26. Нацрта закона прописано је да надлежни орган буде министарство надлежно за послове информационе безбедности. У оквиру својих надлежности ово министарство:

- *припрема и предлаже прописе и планска документа;*
- *води евиденцију оператора ИКТ система од посебног значаја;*
- *врши надзор над радом Канцеларије за информационе технологије и електронску управу у вршењу послова за које је надлежна у складу са овим законом;*
- *врши инспекцијски надзор над применом овог закона и радом оператора ИКТ система од посебног значаја, осим самосталних оператора ИКТ система и ИКТ система за рад са тајним подацима;*
- *остварује међународну сарадњу у оквиру својих надлежности.*

Ипак, ово министарство није одређено за јединствену тачку контакта, већ је чланом 30. Нацрта закона прописано да послове јединствене тачке контакта врши Канцеларија за информационе технологије и електронску управу.

Свака држава чланица треба да одреди или успостави један или више надлежних органа одговорних за управљање великим инцидентима и кризама. Ако се одреди више органа, мора се недвосмислено одредити која институција координира њихов рад у случају великих инцидената и криза. Државе чланице такође морају усвојити национални план за одговор на велике инциденте и кризе који мора садржати:

- циљеве због којих се предузимају мере и активности,
- задатке и одговорности надлежних органа,
- процедуре за реаговање и њихово уклапање у општи оквир за реаговање у случају националне кризе, као и канале за размену информација,
- мере које је потребно предузети ради припреме, укључујући вежбе и обуке,
- организације из јавног и приватног сектора и инфраструктуру која се ангажује,
- процедуре и споразуме између националних надлежних органа.

Инциденти у ИКТ системима од посебног значаја класификовани су у члану 16. Нацрта закона у четири категорије: низак, средњи, висок и веома висок. Канцеларија за информационе технологије и електронску управу управља одговором на инциденте ниског, средњег и високог нивоа у сарадњи са операторима ИКТ система од посебног значаја, министарством надлежним за послове информационе безбедности, Телом за координацију послова информационе безбедности и другим надлежним органима по потреби. Инциденти веома високог нивоа сматрају се кризом информационе безбедности и у том случају руковођење и координацију спровођења мера и задатака предузима Влада, која на предлог министарства надлежног за послове информационе безбедности доноси одлуку о проглашењу кризе информационе безбедности и задужује органе да поступају према предложеним мерама у складу са својим надлежностима.

Нацртом закона предвиђена је израда Плана за реаговање у случају инцидента високог нивоа и криза информационе безбедности.

НИС 2 Директивом је одређено да свака земља чланица мора успоставити један или више ЦСИРТ-ова који морају покривати све секторе којима припадају оператори есенцијалних сервиса и

сервисе које пружају оператори дигиталних сервиса и бити одговорни за поступање са инцидентима.

Чланом 28. Нацрта закона прописано је успостављање надлежности Канцеларије за информационе технологије и електронску управу. Прописане надлежности Канцеларије за информационе технологије и електронску управу су:

1) *врши превенцију и заштиту од безбедносних ризика на националном нивоу у складу са овим законом (послови Националног ЦЕРТ-а);*
2) *предузима превентивне и реактивне мере у циљу заштите Јединствене информационо-комуникационе мреже електронске управе у складу са овим законом (послови ЦЕРТ-а органа власти);*
3) *обавља сарадњу на националном нивоу у области информационе безбедности;*
4) *врши послове јединствене тачке контакта;*
5) *врши послове сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга, изузев система, производа, процеса и услуга за потребе одбране и безбедности и ИКТ система за рад са тајним подацима;*
6) *прописује минималне мере заштите ИКТ система органа, уважавајући начела из члана 3. овог закона, мере заштите из члана 10. овог закона, националне и међународне стандарде и стандарде који се примењују у одговарајућим областима рада;*
7) *у сарадњи са надлежним органима и другим субјектима из јавног, академског, привредног и невладиног сектора учествује у развоју и спровођењу програма обука и стручног усавршавања лица која раде на пословима информационе безбедности;*
8) *обавља сарадњу и размену информација на међународном нивоу у области информационе безбедности у циљу праћења и усаглашавања са међународним прописима и стандардима;*
9) *врши стручни надзор над радом оператора ИКТ система од посебног значаја;*
10) *води базу рањивости ИКТ производа и ИКТ услуга;*
11) *извештава Министарство на кварталном нивоу о предузетим активностима;*
12) *обавља друге послове у складу са овим законом.*

Регулаторно тело за електронске комуникације и поштанске услуге обавља послове Националног ЦЕРТ-а утврђене овим законом до истека периода од 12 месеци од дана ступања на снагу овог закона. Надзор над радом Канцеларије за информационе технологије и електронску управу врши министарство надлежно за информациону безбедност.

Нацрт закона, као и постојећи Закон о информационој безбедности, препознаје самосталне операторе ИКТ система (министарство надлежно за послове одбране, министарство надлежно за унутрашње послове, министарство надлежно за спољне послове, службе безбедности и Народна банка Србије) који покривају своје ИКТ системе и на које се не примењују одредбе о пријављивању инцидената који значајно угрожавају информациону безбедност и одредбе о достављању статистичких података о инцидентима. Самостални оператор ИКТ система има обавезу да:

1) *поднесе пријаву за упис у евиденцију ИКТ система од посебног значаја;*

2) *предузме одговарајуће техничке, оперативне, организационе и физичке мере заштите ИКТ система од посебног значаја, управљање ризицима и превенцију и смањење штетних последица инцидената;*
3) *донесе акт о безбедности ИКТ система;*
4) *врши проверу усклађености мера заштите ИКТ система које се примењују са актом о безбедности ИКТ система у складу са сопственим правилима за проверу усклађености мера заштите, а најмање једном годишње;*
5) *уреди однос са трећим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом, уколико поверава активности у вези са ИКТ системом од посебног значаја са трећим лицима;*
6) *формира сопствени ЦЕРТ ради управљања инцидентима у својим системима.*

Нацртом закона, чланом 33. препознати су и Посебни ЦЕРТ-ови за превенцију ризика у ИКТ системима који обављају послове превенције и заштите од безбедносних ризика у ИКТ системима у оквиру одређеног правног лица, групе правних лица, области пословања и слично.

НИС 2 Директивом је прописано да ЦСИРТ -ови морају испуњавати следеће захтеве:

- морају обезбедити висок ниво доступности својих комуникационих сервиса избегавањем јединствене тачке прекида и имати увек на располагању више начина да буду контактирани и да они контактирају друге;
- запослени и информациони системи које користе морају бити смештени на безбедним локацијама;
- морају бити опремљени одговарајућим системима за управљање и прослеђивање захтева;
- морају обезбедити поверљивост и поузданост својих операција;
- морају бити попуњени адекватним бројем и квалитетом запослених;
- морају имати осигуран континуитет рада инфраструктуре, укључујући редундантни простор и опрему.

Послови ЦСИРТ-ова морају обухватити:

- праћење и анализирање сајбер претњи, рањивости и инцидената на националном нивоу и, на захтев, пружање помоћи есенцијалним и важним ентитетима,
- пружање раних упозорења и других информација о ризицима и инцидентима есенцијалним и важним ентитетима, надлежним органима и другим субјектима од значаја,
- реаговање на инциденте и пружање помоћи есенцијалним и важним ентитетима (где је применљиво),
- пружање динамичке анализе ризика и инцидената и указивање на тренутну ситуацију,
- пружање есенцијалним и важним ентитетима услуге проактивног скенирања мрежних и информационих система ради откривања рањивости,
- учешће у Мрежи ЦСИРТ-ова,
- координацију активности усмерених на координисано откривање рањивости (где је применљиво), и
- допринос примени безбедних алата за размену информација.

Такође, прописано је да ЦСИРТ-ови промовишу усвајање и употребу уобичајених или стандардизованих пракси, класификационих шема и таксономија у вези са:

- процедурама за решавање инцидената,

- управљањем кризама и
- координисаним откривањем рањивости.

Чланом 29. Нацрта закона прописано је да у оквиру послова превенције и заштите од безбедносних ризика и инцидената Канцеларија врши послове Националног ЦЕРТ-а и то:

1) *прикупља и размењује информације о претњама, рањивостима и инцидентима и пружа подршку, упозорава и саветује лица која управљају ИКТ системима у Републици Србији као и јавност.*
2) *прати стање о инцидентима у Републици Србији;*
3) *пружа рана упозорења, узбуне и најаве и информише релевантна лица о претњама, рањивостима и инцидентима;*
4) *реагује без одлагања по пријављеним или на други начин откривеним инцидентима у ИКТ системима од посебног значаја, као и по пријавама физичких и правних лица, тако што пружа савете и препоруке на основу расположивих информација о инцидентима и предузима друге потребне мере из своје надлежности на основу добијених сазнања;*
5) *на захтев оператора ИКТ система од посебног значаја, пружа помоћ у праћењу стања безбедности ИКТ система у реалном времену или приближно реалном времену;*
6) *на захтев оператора ИКТ система од посебног значаја, врши проактивно скенирање ИКТ система у циљу утврђивања рањивости које могу да потенцијално знатно наруше безбедност ИКТ система, при чему такво скенирање не сме имати штетан утицај на послове и делатности оператора;*
7) *поступа као координатор за потребе координираног откривања рањивости, у складу са овим законом;*
8) *учествује у развоју и коришћењу технолошких алата за размену информација са операторима ИКТ система од посебног значаја и других субјеката са којима сарађује;*
9) *континуирано израђује анализе ризика и инцидената, на основу прикупљених информација;*
10) *подиже свест код грађана, привредних субјеката и органа о значају информационе безбедности, о ризицима и мерама заштите, укључујући спровођење кампања у циљу подизања те свести;*
11) *води Евиденцију посебних ЦЕРТ-ова;*
12) *припрема извештаје на кварталном нивоу о предузетим активностима.*

Поред тога, Канцеларија за информационе технологије и електронску управу подстиче примену и коришћење прописаних и стандардизованих процедура за:

- *управљање и санирање ризика и инцидената,*
- *класификацију информација о ризицима и инцидентима, односно класификацију према нивоу инцидената и ризика,*
- *управљање кризним ситуацијама и*
- *координирано откривање рањивости.*

Чланом 30. Нацрта закона прописано је да Канцеларија за информационе технологије и електронску управу обавља следеће послове у оквиру предузимања превентивних и реактивних мера у циљу заштите Јединствене информационо-комуникационе мреже електронске управе (ЦЕРТ органа власти):

- *врши заштиту мреже еУправе,*
- *обавља координацију и сарадњу са операторима ИКТ система које повезује мрежа еУправе у превенцији инцидената,*

- *активно учествује у откривању инцидената, прикупљању информација о инцидентима и отклањању последица инцидената,*
- *врши проактивно скенирање мреже оператора ИКТ система од посебног значаја који су корисници мреже, при чему такво скенирање не сме имати штетан утицај на послове и делатности оператора,*
- *у случају откривене рањивости:*
    - *обавести операторе ИКТ система који су корисници мреже еУправе о томе,*
    - *налаже операторима ИКТ система од посебног значаја који су корисници мреже да предузму адекватне мере заштите у циљу спречавања, смањења и отклањања последица инцидента*,
- *издаје стручне препоруке за заштиту ИКТ система органа, осим ИКТ система за рад са тајним подацима,*
- *доноси акт којим се уређује поступање оператора ИКТ система од посебног значаја који користе мреже у случају инцидента*,
- *у сарадњи са надлежним органима врши процену потребе за стручним усавршавањем запослених у операторима ИКТ система од посебног значаја који користе мрежу,*
- *планира и организује процедуралне и практичне вежбе у области информационе безбедности за запослене у операторима ИКТ система од посебног значаја који користе мрежу,*
- *израђује предлоге за унапређење безбедносних карактеристика мреже еУправе,*
- *израђује анализе ризика и инцидената у оквиру мреже еУправе,*
- *обавља друге послове у складу са законом у циљу унапређења информационе безбедности мреже еУправе.*

Одредбе о координисаном откривању рањивости су уведене у НИС 2 Директиву као нова тема (која није постојала у НИС Директиви). НИС 2 Директивом прописано је да државе чланице треба да одреде ЦСИРТ који ће бити координатор ових активности. Тај ЦСИРТ треба да делује као посредник од поверења и олакша комуникацију између оног ко пријављује рањивост (било да је у питању правно или физичко лице) и произвођача потенцијално рањивог производа или пружаоца потенцијално рањиве услуге. Задаци овог ЦСИРТ-а укључују:

- идентификацију и успостављање контакта са предметним странама,
- помоћ страни која пријављује рањивост и
- договарање о роковима за објављивање, као и управљање рањивостима које утичу на више ентитета.

Страни која пријављује рањивост мора бити загарантована анонимност ако то жели.

НИС 2 Директива даје задатак ЕНИСА-и да развије и одржава Европску базу рањивости, укључујући одговарајући информациони систем, политике и процедуре, као и да предузме неопходне техничке и организационе мере које ће гарантовати безбедност и интегритет ове базе података. База података ће бити доступна свим значајним ентитетима, а садржаће следеће податке:

- опис рањивости,
- обухваћене производе или услуге и озбиљност рањивости у смислу околности под којима она може бити експлоатисана и
- доступност одговарајуће закрпе или упутство за умањење ризика ако закрпа не постоји.

Чланом 34. Нацрта закона прописано је да Канцеларија за информационе технологије и електронску управу успоставља и одржава базу рањивости ИКТ производа и ИКТ услуга у Републици Србији и омогућава физичким и правним лицима да на добровољној бази пријаве рањивости, као и да то учине анонимно. База рањивости ИКТ производа и ИКТ услуга садржи:

- *податке о рањивости и*
- *податке о ИКТ производима или ИКТ услугама на које рањивост утиче.*

НИС 2 Директивом је прописано да надлежни орган, јединствена тачка контакта и ЦСИРТ-ови једне државе чланице међусобно сарађују у циљу испуњавања обавеза које су им постављене овом Директивом. Ово се посебно односи на размену информација о инцидентима, избегнутим инцидентима и претњама. Такође, прописана је размена информација између надлежних органа успостављених овом Директивом и Директивом 2022/2557.

Нацрт закона прописује сарадњу Канцеларије за информационе технологије и електронску управу, министарства надлежног за информациону безбедност, ЦЕРТ-а мреже еУправе, посебних ЦЕРТ-ова, јавних и привредних субјеката и ЦЕРТ-ова самосталних оператора ИКТ система.

Један од облика сарадње на националном нивоу прописан Нацртом закона је кроз активности Тела за координацију послова информационе безбедности, које је координационо тело Владе и у чији састав улазе представници министарства надлежног за послове информационе безбедности, одбране, унутрашњих послова, спољних послова, правде, представници служби безбедности, Канцеларије за информационе технологије и електронску управу, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата Владе, Народне банке Србије и Регулаторног тела за електронске комуникације и поштанске услуге.

Есенцијални и важни ентитети морају спроводити одговарајуће и пропорционалне техничке, оперативне и организационе мере за управљање ризицима по мрежне и информационе системе које користе за пружање својих услуга. Ове мере морају обухватити најмање:

- политике у вези анализе ризика и безбедности информационих система;
- руковање инцидентима;
- континуитет пословања и управљање кризама;
- безбедност ланца снабдевања;
- безбедност у набавци, развоју и одржавању мрежних и информационих система, укључујући руковање и откривање рањивостима;
- политике и процедуре за процену ефикасности мера за управљање ризиком;
- практиковање основних мера сајбер хигијене и обуке у циљу подизања безбедносне свести;
- политике и процедуре везане за коришћење криптографских метода;
- безбедност људских ресурса, политике контроле приступа и управљање асетима;
- коришћење мултифакторске аутентификације и других метода јаке аутентификације и коришћење безбедних комуникационих система, посебно у случају ванредних ситуација.

Оператор ИКТ система од посебног значаја дужан је да донесе акт о процени ризика за ИКТ системе којима управља, којим се врши процена ризика за ИКТ систем од посебног значаја с обзиром на степен изложености ризику, величину оператора и извесност појаве инцидента и његове озбиљности, као и његов потенцијални друштвени и економски

утицај. Оператор ИКТ система од посебног значаја дужан је да донесе акт о безбедности ИКТ система, којим се одређују се мере заштите, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја.

Овим мерама се обезбеђује превенција од настанка инцидената, односно превенција и смањење штете од инцидената, а оне се односе на:

- *успостављање организационе структуре, са утврђеним пословима, знањима, компетенцијама, искуством и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система;*
- *прикупљање података о претњама по информациону безбедност ИКТ система;*
- *постизање безбедности рада на даљину и употребе мобилних уређаја;*
- *обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност, односно да обезбеди одржавање основних и по потреби напредних информатичких обука за све запослене и ангажована лица која имају приступ ИКТ системима као и специјализоване стручне обуке за запослене одговорне за управљање информационом безбедности ради обезбеђивања континуиране едукације;*
- *обезбеђивање довољно ресурса за адекватно управљање информационом безбедношћу;*
- *заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система;*
- *идентификовање информационих добара и одређивање одговорности за њихову заштиту;*
- *класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. овог закона;*
- *заштиту носача података;*
- *ограничење приступа подацима и средствима за обраду података;*
- *одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа;*
- *утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију;*
- *предвиђање употребе криптографских контрола и других техника за сакривање података ради заштите поверљивости, аутентичности и интегритета података;*
- *примена мера заштите ради спречавања отицања података;*
- *физичку заштиту објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему;*
- *заштиту од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем;*
- *обезбеђивање исправног и безбедног функционисања средстава за обраду података;*
- *примену одговарајућих процедура и мера заштите приликом коришћења услуге рачунарства у клауду;*
- *праћење ИКТ система у циљу откривања рањивости и претњи*
- *ограничење приступа интернет страницама које могу потенцијално да наруше безбедност ИКТ система;*
- *заштиту података и средства за обраду података од злонамерног софтвера;*
- *заштиту од губитка података;*

- *чување података о догађајима који могу бити од значаја за безбедност ИКТ система;*
- *обезбеђивање интегритета софтвера и оперативних система;*
- *заштиту од злоупотребе техничких безбедносних слабости ИКТ система;*
- *обезбеђивање заштите ИКТ система приликом спровођења ревизорског тестирања;*
- *заштиту података у комуникационим мрежама укључујући уређаје и водове;*
- *безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система;*
- *испуњење захтева за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;*
- *заштиту података који се користе за потребе тестирања ИКТ система односно делова система;*
- *процедуре за чување и брисање информација у ИКТ системима, у складу са прописима;*
- *заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга;*
- *одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга;*
- *превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама, као и примену мера санације последица инцидента;*
- *мере које обезбеђују континуитет обављања посла у ванредним околностима које су дефинишу Планом континуитета обављања посла.*

НИС 2 Директива одређује да оператори есенцијалних и важних сервиса, без непотребног одлагања, обавесте надлежни орган или ЦСИРТ о инцидентима који имају или могу имати значајан утицај на континуитет сервиса који пружају, са довољно информација да се може одредити да ли постоји и прекогранични утицај. Параметри који одређују да је инцидент значајан су:

- инцидент је проузроковао или има капацитет да проузрокује озбиљне прекиде пружања услуга или озбиљне финансијске губитке угроженом ентитету, и
- инцидент је утицао или има капацитет да утиче на друга физичка или правна лица путем наношења значајне материјалне или нематеријалне штете.

Нацртом закона прописано је да оператори ИКТ система од посебног значаја имају обавезу да путем јединственог система за пријем обавештења о инцидентима пријаве инциденте који могу да имају значајан утицај на нарушавање информационе безбедности (односно Народној банци Србије или Регулаторном телу за електронске комуникације и поштанске услуге ако су у питању оператори ИКТ система који спадају у њихову надлежност).

Чланом 13. Нацрта закона прописани су критеријуми за одређивање инцидената који могу да имају значајан утицај на нарушавање информационе безбедности:

1) *инциденти који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга;*
2) *инциденти који утичу на велики број корисника услуга, или трају дужи временски период;*
3) *инциденти који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружања услуга, који утичу на обављање послова и вршење услуга*

других оператора ИКТ система од посебног значаја или утичу на јавну безбедност;

4) *инциденти који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;*
5) *инциденти који доводе до неовлашћеног приступа заштићеним подацима чије откривање може угрозити права и интересе оних на које се подаци односе;*
6) *инциденти који су настали као последица инцидента у ИКТ систему оператора приоритетних ИКТ система од посебног значаја који обављају делатности у области дигиталне инфраструктуре, из члана 5. став 2. тачка 1) подтачка (7) овог закона, када ИКТ систем од посебног значаја у свом пословању користи информационе услуге у области дигиталне инфраструктуре;*
7) *инциденти који изазивају или могу да изазову знатну материјалну или нематеријалну штету оператору ИКТ система од посебног значаја и другим физичким и правним лицима.*

Државе чланице могу захтевати од есенцијалних и важних ентитета да користе одређене ИКТ производе, услуге и процесе који су сертификовани према европским шемама сертификације за информациону безбедност усвојеним у складу са Актом о сајбер безбедности (Уредба ЕУ 2019/881).

Чланом 28. Нацрта закона прописано је да Канцеларија за информационе технологије и електронску управу, између осталог, врши послове сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга, изузев система, производа, процеса и услуга за потребе одбране и безбедности и ИКТ система за рад са тајним подацима. У Нацрту закона, осим навођења у овом члану, нема ближих одредница везаних за ову надлежност.

Са друге стране, у Нацрту закона задржано је читаво поглавље из постојећег Закона о информационој безбедности са осам чланова који детаљно обрађују криптобезбедност и заштиту од компромитујућег електромагнетног зрачења.

НИС 2 Директива прописује да државе чланице обезбеде надзор над спровођењем и предузму неопходне мере за обезбеђење усклађености са овом Директивом.

Нацртом закона предвиђено је да инспекцијски надзор над применом овог закона и радом оператора ИКТ система од посебног значаја (осим самосталних оператора ИКТ система и ИКТ система за рад са тајним подацима) врши инспекција за информациону безбедност. Послове инспекције за информациону безбедност обавља Министарство преко инспектора за информациону безбедност. Овлашћења у вези надзора над спровођењем ове Директиве у системима есенцијалних ентитета су:

- инспекције на лицу места и надзор ван локације, укључујући насумичне провере које спроводе обучени стручњаци;
- редовне и циљане безбедносне ревизије које спроводи независно тело или надлежни орган;
- ванредне ревизије, укључујући оне које се спроводе због значајног инцидента или кршења ове Директиве;
- безбедносна скенирања заснована на критеријумима за процену ризика, у сарадњи са предметним субјектом;
- захтеви за информацијама неопходним за процену мера за управљање ризиком;

- захтеви за приступ подацима, документима и информацијама неопходним за обављање надзорних задатака;
- захтеви за доказима о примени политика информационе безбедности.

Државе чланице ће обезбедити да њихови надлежни органи према есенцијалним ентитетима имају овлашћење најмање да:

- издају упозорења о кршењу ове Директиве;
- усвоје обавезујућа упутства, укључујући она у вези са мерама неопходним за спречавање или отклањање инцидента, као и временске рокове за спровођење тих мера и извештавање о њиховој примени;
- наређе предметним субјектима да престану са кршењем одредби ове Директиве;
- наређе предметним субјектима да обезбеде да су њихове мере за управљање ризиком информационе безбедности и извештавања у складу са овом Директивом;
- наложе предметним субјектима да физичким или правним лицима којима пружају услуге пруже обавештења о актуелној претњи, природи претње, као и о свим могућим мерама које могу предузети та физичка или правна лица као одговор на ту претњу;
- наложе предметним субјектима да у разумном року спроведу препоруке дате као резултат ревизије безбедности;
- Одреде службеника за праћење усклађености предметних субјеката са наложеним мерама за управљање ризиком и извештавање;
- наређе предметним субјектима да на одређен начин објаве аспекте кршења ове Директиве;
- наметну или затраже изрицање административне казне.

Овлашћења у вези надзора над спровођењем ове Директиве у системима важних ентитета су:

- инспекције на лицу места и надзор ван локације које спроводе обучени стручњаци;
- циљане безбедносне ревизије које спроводи независно тело или надлежни орган;
- безбедносна скенирања заснована на критеријумима за процену ризика, у сарадњи са предметним субјектом;
- захтеви за информацијама неопходним за процену мера за управљање ризиком;
- захтеви за приступ подацима, документима и информацијама неопходним за обављање надзорних задатака;
- захтеви за доказима о примени политика информационе безбедности.

Државе чланице ће обезбедити да њихови надлежни органи према важним ентитетима имају овлашћење најмање да:

- издају упозорења о кршењу ове Директиве;
- усвоје обавезујућа упутства или налог за отклањање уочених недостатака;
- наређе предметним субјектима да престану са кршењем одредби ове Директиве;
- наређе предметним субјектима да обезбеде да су њихове мере за управљање ризиком информационе безбедности и извештавања у складу са овом Директивом;
- наложе предметним субјектима да физичким или правним лицима којима пружају услуге пруже обавештења о актуелној претњи, природи претње, као и о свим могућим мерама које могу предузети та физичка или правна лица као одговор на ту претњу;
- наложе предметним субјектима да у разумном року спроведу препоруке дате као резултат ревизије безбедности;
- наређе предметним субјектима да на одређен начин објаве аспекте кршења ове Директиве;
- наметну или затраже изрицање административне казне.

Нацртом закона, чланом 45. прописано је да инспектор за информациону безбедност има овлашћења да:

- *наложи отклањање утврђених неправилности и за то утврди разуман рок;*
- *забрани коришћење поступака и техничких средстава којима се угрожава или нарушава информациона безбедност и за то остави рок;*
- *захтева од оператора ИКТ система од посебног значаја да изврши скенирање мреже у циљу утврђивања евентуалних безбедносних рањивости, а у складу са проценом ризика;*
- *наложи да надзирани субјект учини доступним јавности информације које се тичу непоштовања одредби овог закона, а за које постоји оправдан интерес јавности на утврђени начин;*
- *наложи да надзирани субјект одреди лице са тачно утврђеним овлашћењима које ће у утврђеном временском периоду надзирати и пратити усаглашеност са одредбама овог закона и наложеним мерама.*

Измене Закона неопходне су и због доношења Уредбе 881/2019 Парламента и Савета ЕУ о Агенцији Европске Уније за сајбер безбедност (ЕНИСА) (енг. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 - Cybersecurity Act*) која је усвојена 17. априла 2019. године. Уредбом су проширене надлежности ЕНИСА. Ова Уредба значајна је за сертификацију у области информационе безбедности коју је потребно предвидети изменама Закона.

Шема сајбербезбедносне сертификације ЕУ представља свеобухватан сет правила, техничких захтева, стандарда и процедура који је успостављен на нивоу ЕУ и који се односи на сертификацију или процену усаглашености одређених ИКТ производа, сервиса и процеса. Шема националне сајбербезбедносне сертификације односи се на свеобухватан сет правила, техничких захтева, стандарда и процедура развијених и усвојених од стране националних ауторитета и који се односе на сертификацију или процену усаглашености ИКТ производа, сервиса и процеса који спадају у оквир те шеме. Европски сајбербезбедносни сертификат је документ издат од стране релевантне организације којим се потврђује да је одређени ИКТ производ, сервис или процес проверен на испуњавање специфичних безбедносних захтева постављених у шеми сајбербезбедносне сертификације ЕУ.

ИКТ производ представља елемент или групу елемената мрежног или информационог система. ИКТ сервис означава сервис који се у потпуности или углавном односи на пренос, складиштење, преузимање или обраду информација у мрежном или информационом систему. ИКТ процес представља сет активности које се обављају у сврху дизајна, развоја, испоруке или одржавања ИКТ производа или ИКТ сервиса.

Разлог за успостављање оквира за сајбербезбедносну сертификацију је побољшање услова за функционисање интерног тржишта кроз повећање нивоа информационе безбедности и успостављање јединственог приступа сајбербезбедносној сертификацији на нивоу ЕУ. ЕНИСА је Уредбом добила обавезу да до 28. јуна 2020. године објави програм рада по питањима сајбербезбедносне сертификације. Комисија може од ЕНИСА тражити да на основу тог програма направи шему сајбербезбедносне сертификације за кандидата или да преуреди постојећу шему сајбербезбедносне сертификације ЕУ.

Шема треба да обезбеди испуњење следећих циљева:

- Заштиту складиштених, преношених или на други начин обрађиваних података од случајног или намерног складиштења, обраде, приступа или објављивања током целог животног циклуса ИКТ производа, сервиса или процеса;
- Заштиту складиштених, преношених или на други начин обрађиваних података од случајног или намерног уништења, губљења, измене или недоступности током целог животног циклуса ИКТ производа, сервиса или процеса;
- Приступ подацима, сервисима или функцијама само од стране ауторизованих особа, програма или машина и само у мери у којој им је приступ одобрен;
- Идентификацију и документацију познатих зависности и рањивости;
- Бележење свих приступа, коришћења и обраде података, сервиса или функција са свим потребним информацијама;
- Омогућавање провере белешки о приступима, коришћењу и обради података, сервиса или функција;
- Верификацију да ИКТ производи, сервиси и процеси не садрже познате рањивости;
- Благовремено враћање доступности и приступа подацима, сервисима и функцијама у случају физичког или техничког инцидента;
- Безбедност ИКТ производа, сервиса и процеса по дефиницији и по дизајну; и
- Испорука ИКТ производа, сервиса и процеса са ажурним хардвером и софтвером без јавно познатих рањивости и са механизмима за безбедносно ажурирање.

Сразмерно ризику придруженом намени и сврси коришћења и у складу са вероватноћом и утицајем могућег сајбер инцидента, ИКТ производима, сервисима и процесима може се доделити ниво уверења „основни", „знатан" или „висок". „Основни" ниво даје уверење да ИКТ производ, сервис или процес испуњава одговарајуће безбедносне захтеве у погледу минимизације основних ризика од сајбер инцидената и напада, а провера испуњености ових захтева мора укључивати најмање преглед техничке документације. Ниво „знатан" даје уверење да ИКТ производ, сервис или процес, поред критеријума за ниво „основни", испуњава одговарајуће безбедносне захтеве у погледу минимизације познатих ризика од сајбер инцидената и напада и ризике од сајбер инцидената и напада спроведених од стране актера са ограниченим вештинама и ресурсима, а провера испуњености ових захтева мора укључивати најмање проверу да не постоје јавно познате рањивости и проверу да су неопходне безбедносне функционалности коректно имплементиране. Ниво „висок" даје уверење да ИКТ производ, сервис или процес испуњава одговарајуће безбедносне захтеве у погледу минимизације ризика од најсавременијих сајбер напада спроведених од стране актера са значајним вештинама и ресурсима, а провера испуњености ових захтева мора укључивати најмање проверу да не постоје јавно познате рањивости, проверу да су неопходне и најсавременије безбедносне функционалности коректно имплементиране и примену пенетрационих тестирања ради процене отпорности на нападе од стране актера са значајним вештинама.

За ниво уверења „основни", произвођачима је дозвољено да врше самопроцену усаглашености и да самостално издају уверење, при чему сносе потпуну одговорност за сагласност са захтевима.

Свака земља чланица ЕУ у обавези је да одреди један или више националних ауторитета за сајбербезбедносну сертификацију и да о томе обавести Комисију (ако их је више, сваки треба да има своју засебну надлежност). На нивоу ЕУ формираће се Група за европску сајбербезбедносну сертификацију (ECCG) састављена од представника националних ауторитета за сајбербезбедносну сертификацију или других националних ауторитета која ће, између осталог, имати следеће задатке:

- Да саветује и пружи помоћ Комисији у осигурању доследне имплементације програма сајбербезбедносне сертификације;
- Да пружи помоћ, саветује и сарађује са ЕНИСА у припреми шема сертификације;
- Да олакша сарадњу између националних ауторитета за сајбербезбедносну сертификацију кроз изградњу капацитета и размену информација;
- Да олакша прилагођење шема сајбербезбедносне сертификације ЕУ међународно препознатим стандардима итд.

Националне шеме информационе безбедносне сертификације које не спадају у оквир шеме сајбербезбедносне сертификације ЕУ могу да наставе са издавањем сертификата и након ступања на снагу шеме сајбербезбедносне сертификације ЕУ, док оне националне шеме које спадају под овај оквир не смеју више издавати сертификате.

Нацртом Закона у члану 28. су послови сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга поверени Канцеларији за информационе технологије и електронску управу.

5) На које циљне групе ће утицати предложена промена? Утврдити и представити циљне групе на које ће промена имати непосредан односно посредан утицај.

Нови Закон о информационој безбедности имаће непосредан утицај на:

- ИКТ системе од посебног значаја;
- Национални ЦЕРТ;
- ЦЕРТ органа власти - Јединствене информационо-комуникационе мреже електронске управе;
- нове ИКТ системе од посебног значаја;
- ЦЕРТ-ове самосталних оператора ИКТ система.

6) Због чега је неопходно постићи жељену промену на нивоу друштва? (одговором на ово питање дефинише се општи циљ)

Измене националног оквира треба да буду усмерене ка постизању развијеног информационог друштва и електронске управе у служби грађана и привреде, као и унапређену информациону безбедност грађана, јавне управе и привреде, што се постиже:

- побољшањем постојећих и изградњом недостајућих капацитета,
- успостављањем оквира за правовремену и ефикасну размену информација на свим нивоима, а посебно између надлежног органа за информациону безбедност и органа безбедности и одбране,
- координисаном и усклађеном међународном сарадњом,
- усаглашеним моделом образовања и дефинисањем профила људских ресурса у области информационе безбедности,
- ефикасном превентивном и реактивном заштитом критичне информационо-комуникационе инфраструктуре,
- подстицањем истраживачких и развојних капацитета и реализацијом заједничких пројеката јавног, приватног и академског сектора,
- побољшањем информационе безбедности ИКТ система који не спадају у критичну инфраструктуру и становништва у целини,
- успостављањем оквира за безбедносну сертификацију,
- усклађивањем са најбољим праксама, а нарочито са легислативом Европске уније.

Нови Закон о информационој безбедности треба да се донесе првенствено ради потпуног усклађивања са ЕУ регулативом у овој области, а потом ради боље повезаности свих релевантних актера у области информационе безбедности, чиме се доприноси адекватнијем нивоу безбедности информационих система од посебног значаја у Републици Србији, као и подизању информационе безбедности друштва у целини.

Када је реч о ефектима на грађане, треба истаћи да се применом закона очекује следеће:

- већа поузданост услуга које грађани користе путем информационо-комуникационих система од посебног значаја;
- заштита података грађана који се обрађују у ИКТ системима од посебног значаја;
- стварање механизама за подизање свести грађана о значају информационе безбедности;
- успостављање канала путем којих ће грађани моћи да комуницирају са органима у случају проблема и штете који су настали услед нарушавања информационе безбедности;
- обавештавање корисника у случају инцидената који значајно угрожавају ИКТ системе од посебног значаја чије услуге користе и добијање инструкција које мере треба да предузму ради превенције и санирања потенцијалне штете.

7) Шта се предметном променом жели постићи? (одговором на ово питање дефинишу се посебни циљеви, чије постизање треба да доводе до остварења општег циља. У односу на посебне циљеве, формулишу се мере за њихово постизање).

Новим законом преносе се надлежности Канцеларији за информационе технологије и електронску управу, што ће допринети бољој координацији између Министарства и Канцеларије (у којој се обједињавају послови Националног ЦЕРТ-а и ЦЕРТ-а органа власти) са једне стране, али и побољшању сарадње са посебним ЦЕРТ-овима и ИКТ системима од посебног значаја са друге стране.

Такође се предвиђа јачање капацитета Националног ЦЕРТ-а и то технолошких, људских и организационих капацитета, што ће Националном ЦЕРТ-у омогућити прелазак са информативне и саветодавне улоге на оперативнију улогу. Пружајући адекватнију помоћ ИКТ системима од посебног значаја у случају пријављених инцидената, поспешиће се међусобна сарадња и створити поверење што ће последично довести до тога да ИКТ системи од посебног значаја пријављују инциденте у складу са Законом.

Прецизнијим регулисањем појмова (дефиниција) стварају се бољи услови за препознавање и разумевање сајбер претњи.

Давањем већег значаја ЦЕРТ-овима и редефинисањем обавеза оператора информационо-комуникационих система од посебног значаја олакшава се њихово деловање и пружа адекватнији одговор на инциденте.

Израда националног плана деловања у случају великих инцидената утицаће на брже и ефикасније реаговање на сајбер претње.

Унапређење институционалног оквира и побољшање механизама реаговања на инциденте у сајбер простору омогућиће остваривање циљева, и то:

- безбедност информационо-комуникационих система која се односи на ризике нарушавања функционисања органа управе, привреде и организација као последица инцидената у информационо-комуникационим системима и

- информациона безбедност Републике Србије, што се односи на ризике нарушавања националне безбедности путем информационо-комуникационих система.

8) Да ли су општи и посебни циљеви усклађени са важећим документима јавних политика и постојећим правним оквиром, а пре свега са приоритетним циљевима Владе?

Нацрт закона у потпуности је усклађен са Стратегијом развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године. Општим циљем Стратегије ***Развијено информационо друштво и електронска управа у служби грађана и привреде и унапређена информациона безбедност грађана, јавне управе и привреде*** препознат је значај информационе безбедности за друштво у целини. Посебан циљ ***Унапређење информационе безбедности грађана, јавне управе и привреде*** остварује се кроз реализацију следећих мера:

- подизање свести и знања у области информационе безбедности грађана, јавних службеника и привреде,
- подизање капацитета ИКТ система од посебног значаја за примену мера заштите,
- подизање капацитета Националног ЦЕРТ-а, ЦЕРТ-а органа власти и ЦЕРТ-ова самосталних оператора ИКТ,
- подизање капацитета инспекције за информациону безбедност,
- подстицање јавно-приватног партнерства у области информационе безбедности и
- унапређење регионалне и међународне сарадње.

У оквиру мере *Унапређење сарадње и подизање капацитета ИКТ система од посебног значаја за примену мера заштите* предвиђена је посебна активност **Усклађивање прописа са регулативом ЕУ у области информационе безбедности**, што и јесте кључни разлог доношења новог Закона о информационој безбедности. Праћењем европских токова у овој области не врши се само хармонизација прописа, већ и унапређење институционалног оквира и побољшање механизама реаговања на инциденте у сајбер простору, као и превентивног деловања ради очувања информационе безбедности.

9) На основу којих показатеља учинка ће бити могуће утврдити да ли је дошло до остваривања општих односно посебних циљева?

Основни показатељи учинка доношења Закона огледају се у следећем:

- утврђени су начини и механизми за подизање капацитета ИКТ система од посебног значаја
- унапређена је платформа за размену информација између Националног ЦЕРТа и ИКТ система од посебног значаја са механизмом за брзо реаговање
- побољшана је сарадња између ЦЕРТ-ова у Републици Србији и координисан је одговор на кризне ситуације
- број обучених запослених у ЦЕРТ-у органа власти и у самосталним операторима ИКТ се повећава
- број запослених инспектора за информациону безбедност се повећава
- боље је управљање ризиком.

Показатељ	Базна година и вредност	2024	2025	2026
Број организованих сајбер вежби	2023 (1)	2	3	4

Додат број нових функционалности платформи за размену података о инцидентима	2023 (0)	1	2	3
Број састанака ЦЕРТ-ова годишње	2023 (3)	4	5	6
Број полазника обука	2022 (20)	30	40	50
Број запослених инспектора	2023 (2)	3	4	5
Број адекватно сачињених аката о процени ризика	2023 (0)	100	200	300

Усвајање НИС 2 Директиве у децембру 2022. године је био је подстицај да се направи анализа садашњег правног и институционалног оквира, поставе нови циљеви. Нацртом закона остварује се напредак у односу на постојеће стање, како у домену прецизнијег уређивања области, тако и у креирању функционалнијег и ефикаснијег институционалног оквира.

Један од задатака које је Европска унија поставила пред ЕНИСА је и израда оквира за сертификацију производа, сервиса и услуга, који има за циљ да се одреди ниво заштите који могу да пруже одређени производи, сервиси и услуге и да се ојача поверење у дигиталне технологије и провајдере дигиталних сервиса. Нацртом закона уводи се обавеза сертификације ИКТ система која ће се вршити када и европске земље ближе регулишу ово питање.

Без обзира што је позиција Србије у међународних оквирима све боља у овом домену, постоје значајне могућности за побољшање. Међународну сарадњу су остваривали представници Министарства информисања и телекомуникација, РАТЕЛ-а, Министарства спољних послова, Министарства унутрашњих послова и Министарства одбране, што ће се вероватно наставити и у наредном периоду. Важно је да наступи представника Србије у међународним институцијама буду координисани како би могли на најбољи начин да обављају своје послове.

Правовремено откривање и отклањање рањивости је стални изазов на којем заједнички ради више земаља како би се пронашао адекватан начин решавања. Благовременим откривањем претњи јача се степен информационе безбедности као и поверење у институције које се том темом баве.

Нацрт закона уређује оквир за поступање у кризним ситуацијама и заједнички одговор ЦЕРТ-ова.

Поред промоције и подршке учешћу представника институција и организација из Србије на међународним вежбама, ради успостављања одговарајућег одговора на инциденте већих размера неопходна је организација националних сајбер вежби. Ове вежбе треба да организује и спроводи Канцеларија за информационе технологије и електронску управу, а сврха вежби треба да буде провера и увежбавање процедура за реаговање.

Због тога је неопходно развијати партнерске односе са академским институцијама које имају програме за информациону безбедност на основном, мастер и докторском нивоу студија. Канцеларија треба да подстиче научне радове из ових области и учешће академских институција у међународним пројектима јер се на тај начин стичу нова знања и наши академски људски ресурси стимулишу да буду укључени у најновија достигнућа у овој области.

Увођењем механизма сарадње између ЦЕРТ-ова у Републици Србији доприноси се већем степену заштите ИКТ система у свим областима у Републици Србији и бољој координацији у случају

инцидената који могу да угрозе информациону безбедност, али и националну безбедност Републике Србије.

10) Да ли је финансијске ресурсе за спровођење изабране опције потребно обезбедити у буџету, или из других извора финансирања и којих?

Потребно је обезбедити у буџету средства за реализацију обавеза из Закона о информационој безбедности, и то за потребе подизања капацитета Канцеларије за информационе технологије и електронску управу у делокругу послова ЦЕРТ-а органа власти, а због преузимања права, обавеза, запослених, предмета, опреме, средстава за рад и архиве од Регулаторног тела за електронске комуникације и поштанске услуге, који су настали у обављању послова Националног ЦЕРТ-а, потребно је извршити одговарајући пренос финансијских средстава.

11) Колики су процењени трошкови увођења промена који проистичу из спровођења изабране опције (оснивање нових институција, реструктурирање постојећих институција и обука државних службеника) исказани у категоријама капиталних трошкова, текућих трошкова и зарада и да ли је могуће финансирати расходе изабране опције кроз редистрибуцију постојећих средстава?

Будући да је Нацртом закона предвиђено успостављање, односно пренос надлежности на Канцеларију за информационе технологије и електронску управу, то ће захтевати повећавање кадровских и техничких капацитета у наредном периоду, те се предвиђа повећавање броја запослених као и куповина неопходне опреме.

12) Које трошкове и користи (материјалне и нематеријалне) ће изабрана опција проузроковати привреди, појединој грани, односно одређеној категорији привредних субјеката?

ИКТ системи од посебног значаја у области дигиталне инфраструктуре и услуга информационог друштва који су предвиђени изменама и допунама Закона су у обавези да примене мере заштите, односно техничке и организационе мере у циљу успостављања адекватног нивоа безбедности система.

Уколико су ти привредни субјекти већ успоставили систем управљања информационом безбедношћу у складу са међународним стандардима и добром праксом у овој области, не очекује се да примена закона изазове значајне трошкове. Међутим, привредни субјекти који представљају операторе ИКТ система од посебног значаја у складу са новим законом, а који до сада нису успоставили одговарајући систем управљања информационом безбедношћу, имаће одређене трошкове за испуњење законских обавеза који се огледају у евентуалном додатном технолошком опремању, обуци запослених, ангажовању нових стручњака и слично. Прецизни износи додатних трошкова за наведене субјекте варирају у великом распону, будући да исти зависе од више фактора који могу да буду веома различити у различитим привредним субјектима. Наиме, колико ће финансијских средстава за примену закона издвојити ови привредни субјекти зависи од њихове величине, односно броја запослених, технолошке опремљености (поседовање рачунарске опреме, информационог система), обучености запослених за коришћење информационих технологија у домену информационе безбедности, и других фактора од којих функционисање информационе

безбедности зависи у једном привредном субјекту. Сходно наведеном, није могуће дати ни тачне, ни оквирне износе по привредном субјекту.

13) Да ли је за спровођење изабране опције обезбеђена подршка свих кључних заинтересованих страна и циљних група? Да ли је спровођење изабране опције приоритет за доносиоце одлука у наредном периоду (Народну скупштину, Владу, државне органе и слично)?

Министарство информисања и телекомуникација је почетком 2023. године формирало радну групу за израду Нацрта Закона о информационој безбедности кога су чинили представници релевантних министарстава, посебних организација, агенција, академске заједнице и привреде. Током припреме Нацрта одржано је неколико консултација са различитим интересним групама. Са привредом су одржане консултације 22. јуна у Националној алијанси за локални економски развој на којима су представљени предлози текста Нацрта. Састанку је присуствовало близу 20 привредних субјеката.

Министарство информисања и телекомуникација спровело је јавну расправу о Нацрту Закона о информационој безбедности у периоду од 27. јула до 30. августа 2023. године, на основу закључка Владе. У оквиру јавне расправе, одржана су два округла стола у Београду и Крагујевцу. У јавној расправи учествовали представници државних органа, привредног сектора, академске заједнице, невладиних организација и еминентни стручњаци у овој области.

Иако је текст закона незнатно измењен у односу на 2023. годину, у 2024. години из процедуралних разлога поновљена је јавна расправа и то у периоду од 3. јула до 23. јула 2024. године, након које је Министарство објавило извештај о одржаној јавној расправи на сајту Министарства и порталу „еКонсултације“.

Доношење закона је приоритет имајући у виду чињеницу да се истим врши усклађивање са европском регулативом.

14) Које додатне мере треба спровести и колико времена ће бити потребно да се спроведе изабрана опција и обезбеди њено касније доследно спровођење, односно њена одрживост?

Ради реализације закона, предвиђено је доношење следећих подзаконских аката:

- Уредба којом се ближе уређују услови, општи и секторски критеријуми за одређивање оператора приоритетних и важних ИКТ система од посебног значаја;
- Уредба о ближем садржају акта о безбедности ИКТ од посебног значаја, начину провере и садржају извештаја о провери безбедности ИКТ система од посебног значаја;
- Уредба о ближем уређењу мера заштите ИКТ система од посебног значаја;
- Уредба о поступку обавештавања о инцидентима, обрасцима за обавештавање, листи инцидената према врстама и класификацији инцидената према нивоу опасности;
- Уредба о начину спровођења мера за безбедност и заштиту деце на интернету;
- Правилник о подацима које садржи евиденција оператора информационо-комуникационих система од посебног значаја;
- Правилник о општој методологији за процену ризика у ИКТ системима од посебног значаја;

- Правилник о врсти, форми и начину достављања статистичких података о инцидентима у информационо-комуникационим системима од посебног значаја;
- Правилник о садржају, начину уписа и вођењу евиденције посебних центара за превенцију безбедносних ризика у информационо-комуникационим системима;
- Правилник о садржају, процедури верификације рањивости, начина уписа и вођења регистра.

Ради упознавања јавности са новим законским решењима, Министарство информисања и телекомуникација одржаваће посебне скупове на којима ће упознавати сва заинтересована лица о усвојеним одредбама. Посебан фокус ће бити на операторе ИКТ система од посебног значаја, којима се овим законом прописују обавезе у циљу заштите њихових система. Очекује се да ће се ове активности почети да спроводе одмах по доношењу закона, односно подзаконских акта које овај закон предвиђа, и да ће трајати најмање годину дана, а по потреби и дуже.

Међуинституционална сарадња између органа који спроводе овај закон успоставиће се на више начина:

- Кроз рад Владиног Тела за координацију послова информационе безбедности, које окупља све органе чији су послови од великог значаја за информациону безбедност у Републици Србији;
- У поступку обавештавања о инцидентима који значајно угрожавају информациону безбедност у Републици Србији, надлежни органи остварују сарадњу по питању размене информација, посебно ако је реч о инцидентима који представљају кривично дело или угрожавају одбрану и националну безбедност Републике Србије, односно критичну инфраструктуру.

Закон предвиђа и међусобну сарадњу ЦЕРТ-ова (Националног ЦЕРТ-а, ЦЕРТ-а Јединствене информационо-комуникационе мреже електронске управе, Посебних ЦЕРТ-ова и других ЦЕРТ-ова).

15) Да ли су обезбеђена финансијска средства за спровођење изабране опције? Да ли је за спровођење изабране опције обезбеђено довољно времена за спровођење поступка јавне набавке уколико је она потребна?

Средства за реализацију обавеза из Нацрта закона о информационој безбедности обезбеђују се у буџету Републике Србије. Имајући у виду да је за Канцеларију за информационе технологије и електронску управу, која је до сада обављала и наставља да обавља послове ЦЕРТ-а органа власти, предвиђено повећање капацитета, као и да Канцеларија преузима надлежности Националног ЦЕРТ-а, па самим тим и права, обавезе, запослене, предмете, опрему, средства за рад и архиву од Регулаторног тела за електронске комуникације и поштанске услуге до истека 12 месеци од дана ступања на снагу овог закона, потребно је предвидети већи износ у буџету, односно преузети финансијска средства од поменутог органа. Обезбеђено је довољно времена за спровођење јавних набавки, уколико буде потребе за истим.