Стратегија за
сајбер безбедност
2025 – 2028

Содржина

Резиме

Во рамките на процесот на дигитална трансформација на државата, безбедноста на информациските системи (сајбер безбедноста) претставува клучен национален приоритет за заштита на дигиталната инфраструктура и услуги што ги користат граѓаните, државните и јавните институции и економијата.

Динамичниот развој на информациско-комуникациските технологии и нерамномерната дигитализација на процесите во различни димензии на општеството значително ја менува перспективата за сајбер безбедноста и го зголемува ризикот од сајбер напади и сајбер инциденти. Безбедна, отпорна и доверлива дигитална трансформација на процесите, и на општеството во целина, може да се постигне само доколку е поставена на солидни основи, во сигурен и отпорен сајбер екосистем.

Стратегијата за сајбер безбедност 2025 - 2028 на Република Северна Македонија е стратешки документ, чија цел е, преку дијапазон на активности и мерки, да обезбеди безбедна, отпорна и доверлива дигитална средина, која ја прави Република Северна Македонија безбедно место за онлајн дејствување и работа, со напредни човечки и технички капацитети. Водечката премиса на Стратегијата за сајбер безбедност е овозможување услови за координиран национален одговор на предизвиците во поглед на сајбер безбедноста, како и превенција од сајбер инциденти и напади преку изградба на отпорна дигитална инфраструктура и човечки капацитети.

Преку остварувањето на стратешките цели од Стратегијата за сајбер безбедност, се овозможува заштита и промоција на македонските национални интереси во и преку сајбер просторот, поголем економски раст и просперитет на граѓаните. Во време на хибридно војување, не помалку важен е придонесот што безбедната и отпорна сајбер околина го дава за зајакнување на националните капацитети во општата национална безбедност на државата.

Основните начела на кои се темели Стратегијата за сајбер безбедност 2025 - 2028 се:

- Сајбер безбедноста е одговорност на сите;
- Координација, соработка и поддршка на национално и на меѓународно ниво;
- Сајбер безбедност по дизајн;
- Сајбер безбедност заснована на процена на ризици;
- Холистички пристап кон сајбер безбедноста како двигател на развој на општеството.

Методологијата за развој на Стратегијата за сајбер безбедност се темели на Водичот за развој на Национална стратегија за сајбер безбедност на ITU и насоките и алатките на ENISA. Како основа при изработката е земен националниот стратешки документ за периодот 2018 – 2022 година во корелација со проширувањето на областа на темата на сајбер просторот и предизвиците што ги носи повисокото ниво на дигитализација во Република Северна Македонија.

Стратегијата за сајбер безбедност 2025 - 2028 ќе се имплементира во текот на четири години, од 2025 до 2028 година, во согласност со мерките и задачите дефинирани во Акцискиот план, кој е составен документ на Стратегијата за сајбер безбедност 2025 - 2028 година. Стратегијата за сајбер безбедност и Акцискиот план ги дефинираат улогите на различните чинители во сајбер безбедноста, зајакнатата соработка меѓу јавниот и приватниот сектор и менаџирањето со квалитет на стручниот кадар во оваа област на национално ниво.

Во склоп на Акцискиот план, за секоја активност е предвиден индикативен буџет за имплементација во рамките на Стратегијата за сајбер безбедност 2025 - 2028. Средствата за имплементација и следење на Стратегијата за сајбер безбедност 2025 - 2028 година ќе бидат обезбедени во рамките на буџетот на институцијата Носител на активноста, но онаму каде што тоа е дозволено и со користење донаторски средства за поддршка.
Во акцискиот план, за секоја активност се наведени Носител, Вклучени (засегнати) страни, временска рамка за реализаија, буџет, како и Клучни показатели на перформански(успешност) и на цел. Листа на вклучени (засегнати) страни е дадена во точка 9.3 од овој документ.

Имплементацијата на Стратегијата за сајбер безбедност 2025 - 2028 година, нејзиното следење и мониторирање е во надлежност на МДТ. Во процесот на имплементација ќе се вклучат повеќе засегнати страни, од јавниот и од приватниот сектор, академската и истражувачката заедница, невладините институции и други чинители, кои со своето дејствување директно или индиректно се вклучени во сајбер екосистемот.

1. Вовед

Во дигиталната ера, сајбер безбедноста е основен столб на националната безбедност, на економскиот раст и на општествената отпорност. Стратегијата за сајбер безбедност 2025 - 2028 година ја одразува посветеноста на Владата на Република Северна Македонија да гради безбедна и отпорна дигитална средина, како интегрален елемент од процесот на целосна дигитална трансформација на општеството.

Стратегијата за сајбер безбедност 2025 - 2028 година е клучна за дигиталната трансформација во државата. Обезбедува безбедност на мрежите и на информациските системи, поттикнувајќи доверба во дигиталните технологии и промовирајќи иновации во областа на сајбер заштитата. Стратегијата за сајбер безбедност 2025 - 2028 година поставува цел да ги заштитува критичните ИКТ-услуги, системи и производи, мрежната и информациската инфраструктура, обезбедувајќи континуитет на основните услуги. Исто така, ги штити дигиталните права на граѓаните, придонесувајќи за слободно и отворено дигитално општество. Стратегијата за сајбер безбедност 2025 - 2028 година има за цел да промовира еднаквост преку вклучување на сите групи корисници, особено ранливите и ризичните групи, како деца, жени и други групи.

Стратегијата за сајбер безбедност 2025 - 2028 година придонесува не само во процесот на одбрана од сајбер закани, туку преку проактивна превентивна заштита, работи на овозможување безбедна, издржлива и просперитетна дигитална држава, подготвена да ги прифати можностите и предизвиците што со себе ги носи дигиталната ера.

1.1. Основ за подготвување и предлагање на Стратегијата за сајбер безбедност

Основот за донесување на Стратегијата за сајбер безбедност 2025 - 2028 година не е утврден во посебен акт или документ. Предлагачот на нацрт планскиот документ подготви информација во која ќе се презентира потребата од изработка и донесување на предметната стратегија. Потребата произлегува од Национална стратегија за сајбер безбедност 2018-2022, која Владата на Република Северна Македонија ја усвои на 107 седницата одржана на 11.12.2018 година. Стратегијата за сајбер безбедност 2025 - 2028 година се предлага во насока за континуитет на заложбите на Владата на Република Северна Македонија во областа сајбер безбедност. Согласно Законот за изменување и дополнување на Законот за организација и работа на органите на државната управа, член 26-а, (Службен весник на Република Северна Македонија“ бр. 121/24), Министерството за дигитална трансформација има надлежности во областа безбедност на мрежи и информациски системи.

1.2. Поврзаност со други стратегии во областа и сродни области

Во конкретната област сајбер безбедност, не се идентификувани постојни стратегиски плански документи со исклучок на Националната стратегија за сајбер безбедност 2018-2022.

1.2.1. Национална развојна стратегија (2024-2044)

Стратегијата за сајбер безбедност 2025 - 2028 година и Националната развојна стратегија (НРС) за 2024-2044 година се тесно поврзани преку комплементарните цели за одржлив, безбеден и отпорен развој на Република Северна Македонија. Двете стратегии ги делат заедничките принципи на инклузивност, одржливост, дигитална трансформација и отпорност на современите закани. Усогласеноста се изразува во неколку клучни аспекти:

- Безбедност и отпорност на општеството: Една од клучните стратешки области во НРС е „Сигурно, безбедно и отпорно општество“ што вклучува безбедност на информациските системи и заштита на критичната инфраструктура, опфатени во Стратегијата за сајбер безбедност 2025 - 2028 година. И двете стратегии го нагласуваат управувањето со ризици, подобрување на отпорноста на системите и зајакнување на националните капацитети за заштита од сајбер и хибридни закани.
- Дигитална трансформација и човечки капитал: НРС ја дефинира дигиталната трансформација како централна компонента на развојот, додека Стратегијата за сајбер безбедност 2025 - 2028 година ги поставува основите за безбедна дигитална средина која ги поддржува економските, образовните и административните трансформации. Обуката на кадар, развојот на дигитални вештини и подигањето на свеста за сајбер безбедноста се заеднички приоритети во двете стратегии.
- Владеење на правото и добро управување: Стратешката област на НРС „Владеење на правото и добро управување“ ја изразува потребата од ефикасно управување со сајбер безбедноста, што е клучен елемент во Стратегијата за сајбер безбедност 2025 - 2028 година преку воспоставување на јасни структури за управување, како што е Националниот совет за дигитална трансформација на општеството.
- Социјална инклузија и заштита: НРС ја нагласува важноста на социјалната инклузија, која се огледува во Стратегијата за сајбер безбедност 2025 - 2028 годинапреку заштита на ранливите групи, како што се децата и младите, преку програми за сајбер едукација и безбедност на интернет.
- Меѓународна соработка и интеграција: Двете стратегии истакнуваат меѓународна соработка како критичен фактор. НРС го потенцира стремежот за европска интеграција и усогласување со ЕУ политики, додека Стратегијата за сајбер безбедност 2025 - 2028 годинанагласува партнерства со ЕУ и НАТО за справување со сајбер закани.

Стратегијата за сајбер безбедност 2025 - 2028 годинаи Националната развојна стратегија се комплементарни документи кои се надополнуваат и синхронизираат за да овозможат трансформација на Република Северна Македонија во одржлива, дигитална и безбедна држава. Поврзаноста се рефлектира преку заедничките области на дејствување, како што се отпорност, дигитализација, владеење на правото и социјална инклузија, обезбедувајќи усогласен пристап за постигнување на развојните и безбедносните цели на државата.

1.2.2. Програма за Националната развојна стратегија (НРС) 2024-2028

Стратегијата за сајбер безбедност 2025 - 2028 годинае усогласена со Програмата за Националната развојна стратегија (НРС) 2024-2028 преку заедничките цели за одржлив развој, дигитална трансформација и зајакнување на националните капацитети. Овие две стратегии споделуваат комплементарни цели во неколку клучни области:

- Економија базирана на знаење, иновации и дигитализација: НРС во Стратешката цел 1.1 ги дефинира економскиот раст базиран на дигитализација и иновации, кои се поддржани од Стратегијата за сајбер безбедност 2025 - 2028 годинапреку креирање сигурна и безбедна дигитална инфраструктура. Двете стратегии нагласуваат развој на стартап екосистеми и претприемништво, што е од суштинско значење за економскиот просперитет и безбедност.
- Отпорна критична инфраструктура: Програмата за НРС нагласува важноста на отпорна капитална инфраструктура во функција на подобар живот. Стратегијата за сајбер безбедност 2025 - 2028 година ја поддржува оваа цел преку мерки за заштита на критичните инфраструктури од сајбер-напади.

- Интеграција на дигитални технологии: Во НРС е наведена дигитализацијата како централен двигател за ефективно управување и намалување на нееднаквостите. Стратегијата за сајбер безбедност 2025 - 2028 годинаго поддржува ова преку иницијативи за јакнење на сајбер-капацитетите и промовирање на дигитална доверба во јавниот и приватниот сектор.
- Подобрување на човечкиот капитал: НРС нагласува развој на квалификувана работна сила за потребите на идниот пазар на труд. Стратегијата за сајбер безбедност 2025 - 2028 годинаги комплементира овие цели преку обуки за сајбер-вештини, што е од клучно значење за градење на квалификуван кадар и подобрување на вработливоста.
- Меѓународна соработка и интеграција: И двете стратегии ја потенцираат важноста на меѓународната соработка за поттикнување на економскиот и безбедносниот развој. НРС ја нагласува интеграцијата во глобалните економски синџири, додека Стратегијата за сајбер безбедност 2025 - 2028 година промовира партнерства со ЕУ и НАТО за справување со сајбер закани и инциденти.

1.2.3. Одлуката за стратешки приоритети на Владата (2024-2028)

Стратегијата за сајбер безбедност 2025 - 2028 година) е усогласена со стратешките приоритети на Владата на Република Северна Македонија (2024-2028), согласно Одлуката, со посебен акцент на дигитализацијата, иновациите, безбедноста и владеењето на правото. Преку заедничките цели и активности, се обезбедува интегриран пристап за јакнење на дигиталната и институционалната отпорност.

- Професионална и ефикасна јавна администрација, развој на дигиталната економија, ИКТ секторот, вештачката интелигенција, иновациите и стартап екосистем.

Поврзаност преку целта „воспоставување на стратешка, институционална и законска рамка за обезбедување на сајбер безбедно општество“, која е основа за реализација на стратешкиот приоритет за професионална и ефикасна јавна администрација, дигитална економија и ИКТ секторот. Стратегијата за сајбер безбедност 2025 - 2028 годинаја поддржува оваа цел преку развој на јасна институционална рамка, вклучувајќи формирање на Сектор за сајбер-безбедност во Министерството за дигитална трансформација, поттикнување иновации и употреба на вештачка интелигенција за управување со сајбер ризици и заштита на податоци, како и обезбедување сигурна основа за развој на стартап екосистеми преку унапредување на јавно-приватната соработка за заштита од сајбер закани.

- Обновување на довербата во институциите, зајакнување на безбедноста, ефикасна борба против корупцијата и криминалот, независност на правосудството и обезбедување на владеење на правото

Поврзаност: Стратешкиот приоритет на Владата на Република Северна Македонија го вклучува „јакнењето на сајбер безбедноста и отпорноста на институциите“, со цел заштита на критичната инфраструктура и јакнење на довербата во јавните служби. Стратегијата за сајбер безбедност 2025 - 2028 годинаги адресира овие аспекти преку унапредување на правната рамка за сајбер-безбедност за подобрување на транспарентноста и интегритетот, спроведување мерки за управување со ризици и заштита на критични сектори како енергетиката и здравството, и поттикнување меѓународна соработка за справување со сајбер криминал и транснационални закани.

1.2.4. Стратегијата за отпорност на хибридни закани (2021 – 2025)

Стратегијата за градење отпорност и справување со хибридни закани (2021-2025) ги разгледува современите закани, кои комбинираат воени и невоени методи за постигнување стратегиски цели од страна на државни и недржавни актери. Овие закани вклучуваат дезинформации, сајбер-напади, економски притисоци, злоупотреба на идеологии и култура, како и манипулации преку информативни операции. Стратегијата е фокусирана на шест оперативни области: политика, економија, одбранбено-безбедносен сектор, граѓанскисектор, информативен сектор и критична инфраструктура. Во секоја област се идентификувани конкретни цели, како што се континуитет на владините услуги, енергетска и економска независност, и зголемена медиумска писменост. За справување со овие закани, стратегијата се заснова на интегриран пристап кој комбинира национални капацитети, меѓусекторска координација и меѓународна соработка, со посебен акцент на НАТО и ЕУ иницијативите.
Превенцијата од хибридни закани, како што е нагласено во стратегијата, се базира на три главни столба: рана детекција, намалување на ранливостите и градење на капацитети за одговор и опоравување. Преку системи за детекција на дезинформации, зајакната сајбер-безбедност и управување со ризици, државата има за цел да ги намали потенцијалните влијанија на хибридните закани врз критичните инфраструктури и институции. Дополнително, стратегијата поттикнува јавна едукација и медиумска писменост за намалување на ефектите од дезинформациите, како и развој на законодавни рамки за заштита на критичните сектори. Оваа превенција е поддржана од меѓународни партнерства со НАТО и ЕУ, кои обезбедуваат ресурси за обука, стратешки комуникации и размена на информации.
Стратегијата за сајбер безбедност 2025 - 2028 година и Стратегијата за хибридни закани (2021-2025) се комплементарни, бидејќи и двете препознаваат сајбер-нападите како клучен инструмент на хибридните закани. Хибридните закани, често таргетираат критични инфраструктури преку сајбер-просторот, вклучувајќи сектори со висока критичност. Стратегијата за сајбер безбедност 2025 - 2028 годинасе фокусира на градење силен национален сајбер-екосистем преку јакнење на институционалните капацитети, подобрување на одговорот на инциденти и поттикнување на јавна и приватна соработка. Од друга страна, Стратегијата за хибридни закани го вклучува сајбер-просторот како клучна компонента во заштитата на критичните национални сектори, нагласувајќи ја потребата од меѓународна соработка со НАТО и ЕУ за заедничко справување со сајбер и хибридните предизвици.

1.2.5. Стратегија за паметна специјализација на Република Северна Македонија (2024-2027)

Стратегијата за сајбер безбедност 2025 - 2028 година е комплементарна и усогласена со Стратегијата за паметна специјализација (С3-МК) преку приоритетите за дигитална трансформација, иновации и одржлив економски раст. Овие стратегии споделуваат визија за интеграција на сајбер безбедноста како основа за развој на иновацискиот екосистем, што е суштински за поддршка на критичните приоритетни домени дефинирани во С3-МК.

- Дигитална трансформација и развој на ИКТ секторот: С3-МК ја идентификува дигиталната трансформација како клучна за конкурентноста на економијата и развојот на секторот за информатички и комуникациски технологии (ИКТ). Стратегијата за сајбер безбедност 2025 - 2028 годинаја поддржува оваа визија преку обезбедување сигурна инфраструктура за дигиталните платформи и мрежи, што е неопходно за имплементација на дигитализацијата.
- Иновации и истражувачки капацитети: С3-МК ја нагласува потребата од зајакнување на истражувачките и иновациските капацитети како темел за развој на економија базирана на знаење. Стратегијата за сајбер безбедност 2025 - 2028 годинаго поддржува ова преку развој на иновативни решенија за заштита од сајбер ризици и вклучување на напредни технологии како вештачка интелигенција во истражувачкиот екосистем.

- Поттикнување на зелената и дигиталната транзиција: СЗ-МК промовира интеграција на зелена и дигитална трансформација за одржлив развој, вклучувајќи паметни згради, одржливи материјали и паметно земјоделство. Стратегијата за сајбер безбедност 2025 - 2028 година обезбедува безбедносна рамка за дигиталните технологии кои се основа за имплементација на зелените иницијативи и циркуларната економија.
- Поддршка на иновацискиот екосистем и стартапи: СЗ-МК ја истакнува потребата од создавање стартап екосистем како катализатор за економски раст. Стратегијата за сајбер безбедност 2025 - 2028 година го поддржува развојот на стартапите преку промоција на безбедни дигитални иновации и заштита на интелектуалната сопственост.

Овие стратегии обезбедуваат основа за развој на економијата базирана на знаење, иновации и сигурни дигитални системи, што е клучно за одржливиот раст и интеграцијата на Република Северна Македонија во европскиот и глобалниот пазар.

2. Методологија на Стратегијата за сајбер безбедност

Стратегијата за сајбер безбедност 2025 - 2028 годинае изработена во согласност со методологијата од Водичот за развивање Национална стратегија за сајбер безбедност – изработен од ITU[i], при што се земени предвид и постојните насоки и алатки за изработка на национални стратегии за сајбер безбедност на ENISA[ii].

Стратегијата за сајбер безбедност 2025 - 2028 година ги користи искуствата од Националната стратегија за сајбер-безбедност 2018–2022, како и Акцискиот план, предложените активности и насоки, и е изработена од меѓусекторска работна група под раководство на Министерството за дигитална трансформација. Работната група е формирана со Решение број 08-503/1 од 30.08.2024 година и вклучува членови од следните институции: МДТ, МВР, МНРНТ, МО, АРСМ, УГД Воена академија – Скопје, АЕК, АНБ, АЗЛП, АР, ДБКИ, ОТА, ДЗР и УГД Штип. Преку редовни работни состаноци, членовите на работната група дадоа активен придонес во изработката на овој документ.

При изработка на Стратегијата за сајбер безбедност 2025 - 2028 година, земена е предвид и Информацијата за стандардизација на процесот на подготовка на секторските стратегии со методологија за начинот на подготвување, спроведување, следење, известување и оценување на секторските стратегии[iii] изработена од Владата на Република Северна Македонија, како и Патоказот за дигитална трансформација на општеството.[iv]

Дополнително, Стратегијата за сајбер безбедност 2025 - 2028 година се стреми кон усогласување на активностите поврзани со сајбер безбедност, со европските директиви 2022/2555[v] и 2022/2557[vi], како и со регулативата на ЕУ (881/2019 – Cybersecurity Act)[vii].

Список на користена документација при изработката на Стратегијата за сајбер безбедност 2025 - 2028 година е даден во Анекс 5 – Список на користени информации и референци.

2.1. Опис на процесот на вклучување на засегнатите страни во подготвувањето на стратегијата

Нацрт текстот на планскиот документ, заедно со соодветниот Акциски план, беше поставен на Електронскиот национален регистар на прописи на Република Северна Македонија (ЕНЕР) на 15.10.2024 година. Ова беше направено со цел информирање на сите засегнати страни и овозможување на доставување на коментари и мислења.

Дополнително, по истекот на рокот од 20 дена за доставување коментари и мислења преку ЕНЕР, на 01.11.2024 година, беше одржана јавна расправа за нацрт текстот на планскиот документ со Акцискиот план во Владата на Република Северна Македонија. На оваа расправа учесниците имаа можност да изразат свои ставови и предлози.

3. Анализа на состојбите во секторот сајбер безбедност

Цел на анализата е да се процени тековната состојба на капацитетите за сајбер безбедност во земјата и да се предложат стратешки решенија што се усогласени со стандардите на ЕУ и со глобалните најдобри практики. Цел е да се истакне важноста на меѓународната соработка, законската рамка и градењето капацитети како основни столбови за развој на отпорен сајбер безбедносен екосистем.

3.1. Тековна состојба на сајбер безбедноста во Република Северна Македонија

Република Северна Македонија се соочува со зголемен број сајбер напади, насочени кон критични сектори какви што се енергетика, финансии, водоснабдување и здравство. Високопрофилните инциденти, како нападот врз Министерството за земјоделство, шумарство и водостопанство во 2022 година[viii], нападот врз Фондот за здравствено осигурување од 2023[ix] и нападот врз МЕПСО оваа година[x], предизвикаа значителни нарушувања во јавните услуги, што ги изнесе на површина и ги направи видливи ранливостите на овие сектори.

Наодите од Државниот завод за ревизија на Република Северна Македонија објавени во извештајот „Ефективност на преземените мерки на надлежните органи за заштита на критичните информациски системи“[xi] од 2024 година покажуваат значајни недостатоци во мерките за заштита на критичните информациски системи. Ревизијата утврди дека институциите немаат соодветни законски рамки за да обезбедат целосна сајбер безбедност, бидејќи националното законодавство сè уште не е усогласено со директивите на Европската Унија НИС (2016) и НИС2 (2023), кои поставуваат минимални стандарди за сајбер безбедност. Иако постоеше национална стратегија за сајбер безбедност до 2022 година, нејзината имплементација не е целосно реализирана. Во извештајот се посочува и на недоволната активност на Националниот совет за сајбер безбедност, формиран во 2019 година. Ревизијата утврди дека Советот од неговото формирање до периодот на известување од ревизијата, се состанал само еднаш. Исто така, ревизијата покажа дека институциите немаат доволно технички и административни капацитети за заштита од сајбер инциденти. Недостигот на обучен кадар и тимови за одговор на инциденти, како и отсуството на процена на ризици, ги зголемува ранливостите на критичните системи.

И покрај порастот на финансирањето за сајбер безбедност за 41,68 % во 2023 година, институциите сè уште не успеваат да ги спроведат потребните мерки за целосна заштита, а бројот на пријавени инциденти останува низок. Ревизијата дава препораки за итни реформи, вклучувајќи:

- усогласување на законодавството со директивите на ЕУ,
- подобрување на координацијата меѓу институциите и создавање посилни тимови за сајбер безбедност,
- континуирано вложување во обука и развој на капацитети,

со цел да се избегнат потенцијалните ризици од сајбер напади, кои би можеле да го нарушат функционирањето на клучните сектори какви што се енергетиката, здравството и транспортот.

3.1.1. Управување со сајбер безбедност

Во периодот од 2019 – 2023 година, имаше неколку иницијативи за донесување законско решение за сајбер безбедност, со последен обид во 2023 година, преку објавена работна верзија на Закон за безбедност на мрежи и информациски системи и дигитална трансформација од септември 2023 година, документ што јавно е достапен на ЕНЕР[xii].
На секторско ниво, секторите за енергетика, банкарство и јавни електронски комуникациски мрежи и услуги се единствените што имаат секторска правна рамка што вклучува дефинирање мерки и контроли поврзани со информациска или сајбер безбедност, како и супервизија над имплементирањето од организациите оператори во овие сектори.

Во декември 2018 година, Владата на Република Македонија ја усвои Првата национална стратегија за сајбер безбедност[xiii] што го покриваше периодот од 2018 – 2022 година. Државата е веќе во втора година без стратешки документ што ќе даде насоки за подобрување на отпорноста на сајбер напади и инциденти.

Министерството за дигитална трансформација (во натамошниот текст: МДТ) како наследник на претходното Министерство за информатичко општество и администрација, е основано со измените и дополнувањата на Законот за организација и работа на органите на државната управа[xiv] (во натамошниот текст: ЗОРОДУ), донесени на 10 јуни 2024 година и објавени во „Службен весник на Република Северна Македонија“ бр. 121/24. Во согласност со овие измени, Министерството за информатичко општество и администрација (во натамошниот текст: МИОА) е поделено на две министерства, МДТ и Министерство за јавна администрација. Во споредба со надлежностите што во делот на дигитализацијата ги имаше Министерството за информатичко општество и администрација, новина се следните надлежности, кои директно или индиректно се поврзани и со дигитализација и со сајбер безбедност:

- технолошкиот развој и технолошката култура;
- подготвување стратешки документи од областа на дигитализацијата;
- организирање и спроведување обуки за дигитални вештини;
- безбедност на мрежи и информациски системи;
- дигитализација на јавните услуги;
- администрирање со интегрирана база на лични податоци на населението на Републиката и соодветните книги за евиденција.

Од сите наведени надлежности, безбедноста на мрежи и информациски системи е целосно нова надлежност, додека останатите непосредно или посредно беа дел од портфолиото на МИОА.

3.1.2. Одговор на инциденти

Националниот тим за одговор на компјутерски инциденти (МКД-ЦИРТ[xv]) е одговорен за инциденти на национално ниво, но се соочува со ограничени ресурси и треба да се зајакне за да одговори на растечкиот дијапазон на закани. И покрај неколку најави за формирање дополнителни CSIRT тимови, во моментов нема јавно достапни информации за други оперативни тимови на секторско или организациско ниво во државата.
Националните сајбер безбедносни вежби, како што е Националната координациска вежба за сајбер безбедност 2023, откриja значителни недостатоци во капацитетите за откривање и одговор на сајбер инциденти. Координацијата помеѓу секторите останува критичен аспект за подобрување, како и недостигот на ресурси и тимови за брз, стручен и квалитетен одговор по случен сајбер инцидент или при сајбер напади.
Иако националната и секторските законски рамки за сајбер безбедност се развиваат во насока за усогласување со директивите на ЕУ, недостасува нивно спроведување и ажурирање поврзани

со заштита на критичната инфраструктура, дигиталните услуги и сајбер безбедноста во јавниот сектор.

3.2. Стратешки недостатоци и можности

Клучни недостатоци:

- Недостиг на стручна работна сила: Република Северна Македонија нема доволно обучени сајбер безбедносни професионалци. Дополнително, има недостиг на формални и професионални стручни едукативни програми за создавање на овој кадар.
- Проблеми со координацијата на национално ниво и кај голем дел од секторите со висока критичност: Слабата координација помеѓу владиниот и приватниот сектор и меѓународните организации претставува критичен предизвик.
- Недоволни правни одредби: Постојната законска рамка треба да се надгради и да се ажурира, за да ги покрие современите сајбер безбедносни предизвици и да осигури нивно спроведување.

Можности:

- Изградба на капацитети: Преку координиран внатрешен пристап, и преку соработка со меѓународни партнери какви што се НАТО и ЕУ, да се воспостават програми за обука за развој на квалификувана работна сила.
- Јавно-приватни партнерства: Зајакнување на соработката меѓу јавниот и приватниот сектор може значително да помогне и да ја подобри националната сајбер безбедност.
- Подобрување на законската рамка: Со модерна законска рамка што ќе се заснова, пред сè, на директивите на ЕУ вклучително NIS2, и преку посветеност на нејзино спроведување, државата ќе може да ја изгради и континуирано да ја подобрува сајбер безбедноста и заштитата на критичната инфраструктура.

3.3. Препораки

Следуваат препораки од оваа анализа, кои се вклучени во целите, мерките и активностите во Стратегијата за сајбер безбедност 2025 - 2028 година:

- Анали за и изработка на Национален план и програма за системски пристап кон едукација, вработување, задржување и развој на кадар за сајбер безбедност, со цел воспоставување сеопфатна образовна рамка, која ќе вклучува сајбер безбедносни курикулуми за основно, средно и високо образование, преку преточување меѓународни искуства од други земји. Дополнително е потребна анализа на потребите од стручен кадар и план за вработување и развој.
- Подобрување на механизмите за одговор на инциденти. Цел е изградба на мрежа од тимови за одговор на инциденти, кои ќе бидат квалитетно екипирани и кои координирано и ефикасно ќе одговорат на инцидентите и на заканите.
- Јавни кампањи за подигање на свеста, со цел подобрување на сајбер хигиената во државата и едукација на јавноста за добри практики за сајбер безбедност.
- Зајакнување на законската рамка. Донесување законско решение што ќе биде дедицирано на сајбер безбедност, ќе овозможи дефинирање обврски за имплементација и надзор на мерки и контроли за заштита на секторите со висока критичност и услугите и системите на Владата на Република Северна Македонија. Ова законско решение ќе овозможи еднозначно утврдување на улогите и на функциите во Националната рамка за сајбер безбедност.

- Поттикнување на меѓународната соработка, со цел да се овозможи навремена размена на корисни информации за закани, ризици и инциденти, како и координиран меѓународен пристап во одговор и справување со меѓугранични инциденти и напади.

4. Стратешка рамка

Стратешката рамка обезбедува структуриран пристап за постигнување на целите на Стратегијата за сајбер безбедност 2025 - 2028 година, со посебен акцент на одредена цел или на збир на цели. Стратешката рамка претставува сеопфатен план што ги прикажува визијата, начелата, стратешките приоритети и цели, како и активностите што се дел од Стратегијата за сајбер безбедност 2025 - 2028 година. Ги идентификува и ги опишува активностите на сите засегнати страни, вклучително и организациите од владиниот и од приватниот сектор, како и операторите (суштински и важни субјекти) од секторите со висока критичност и други критични сектори во земјата, во нивните напори за подобрување на сајбер безбедноста.

4.1. Визија

„СОЗДАВАМЕ БЕЗБЕДНА ДИГИТАЛНА ИДНИНА ПРЕКУ САЈБЕР БЕЗБЕДНОСТ КОЈА ГО ПОТТИКНУВА ПРОЦЕСОТ НА ДИГИТАЛНА ТРАНСФОРМАЦИЈА ВО РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА!“

4.2. Приоритетни области, општи и посебни цели во секоја од приоритетни области

Основните начела на кои се темели Стратегијата за сајбер безбедност 2025 - 2028 годинасе следните:

1. **Сајбер безбедноста е одговорност на сите**: Промовирање колективна и индивидуална одговорност за создавање и одржување зрела сајбер безбедносна култура. Интеграција и координација на напорите поврзани со сајбер безбедноста низ владиниот и приватниот сектор. Сеопфатен и координиран пристап во градењето на сајбер отпорноста и интеграцијата и координацијата на напорите низ владиниот и приватниот сектор, академската заедница и граѓанскоиот сектор и централизирани политики и организации со споделени обврски. Воспоставување, одржување и надградба на ИКТ-инфраструктура отпорна на сајбер закани според утврдени стандарди.
2. **Соработка и поддршка на национално и на меѓународно ниво**: Изградба и вклученост во заемни корисни активности на јавниот и на приватниот сектор, како што е споделување информации и научени лекции по однос на сајбер безбедноста и подобрување на заштитата од заеднички закани. Промоција на култура на сајбер безбедност кај граѓаните, кај јавниот и приватниот сектор, во смисла на разбирање на ризиците, сајбер хигиена, превенција и справување со заканите. Меѓународна соработка и дипломатија за сајбер безбедност, што вклучува размена на добри практики.
3. **Сајбер безбедност по дизајн**: Обезбедување упатства, управување и надзор за да се обезбеди исполнување на барањата за сајбер безбедност при планирање,

дизајнирање, развој, имплементација и управување со информациските системи. Градење и унапредување на потребните капацитети за заштита.

4. **Сајбер безбедност заснована на процена на ризици**: Фокус на идентификување, приоритизирање и справување со најкритичните закани врз основа на нивното потенцијално влијание. Преку јакнење на ресурсите и на способностите на државата за континуирано оценување на ризиците, ќе се обезбеди фокусирано и ефикасно распределување на ресурсите за заштита од сајбер напади и закани. Јасно идентификување и дефинирање на изворите на закана по националните интереси во смисла на сајбер безбедноста, превенција и развој на јасен одговор на сајбер криминалот.

5. **Холистички пристап кон сајбер безбедноста**: Примена на интегративен и сеопфатен метод за заштита на информациските системи, мрежи и податоци. Овој пристап ги вклучува технологиите, процесите и луѓето за да се обезбеди целосна заштита и одржување на сајбер безбедноста.

Петте приоритени области, општи и посебни цели чие исполнување води до остварување на визијата на Стратегијата за сајбер безбедност 2025 - 2028 година, се следните:

- ПРИОРИТЕТНА ОБЛАСТ 1: Силни национални капацитети за сајбер безбедност.
    - ОПШТА ЦЕЛ: Обезбедување на отпорен и сигурен национален сајбер простор.
        - ПОСЕБНА ЦЕЛ 1. Јасна и робусна структура за управување со сајбер безбедноста
        - ПОСЕБНА ЦЕЛ 2: Формирање на Сектор за сајбер безбедност во МДТ
        - ПОСЕБНА ЦЕЛ 3. Зголемени капацитети за одбранбени операции во сајбер просторот
- ПРИОРИТЕТНА ОБЛАСТ 2: Безбедност и отпорност на суштински и важни субјекти, мрежи и информациски и комуникациски системи.
    - ОПШТА ЦЕЛ: Обезбедување на безбедноста, доверливоста и отпорноста на критичните мрежи, информациски системи и суштинските и важни субјекти.
        - ПОСЕБНА ЦЕЛ 1. Управување и следење ризици и закани
        - ПОСЕБНА ЦЕЛ 2: Безбедни и отпорни суштински и важни субјекти
        - ПОСЕБНА ЦЕЛ 3. Подобрена безбедност на националните мрежи и информациски системи
        - ПОСЕБНА ЦЕЛ 4. Препораки за употреба на безбедносната технологија во општеството
        - ПОСЕБНА ЦЕЛ 5. Партнерство и соработка помеѓу државните и приватните капацитети.
- ПРИОРИТЕТНА ОБЛАСТ 3: Општество отпорно на сајбер закани.
    - ОПШТА ЦЕЛ: Создавање свесно и отпорно општество.
        - ПОСЕБНА ЦЕЛ 1. Зголемување на свесноста за сајбер безбедноста и дезинформации во сајбер просторот
        - ПОСЕБНА ЦЕЛ 2. Заштита на деца и млади на интернет.
- ПРИОРИТЕТНА ОБЛАСТ 4: Минимизирање на влијанието на инциденти во сајбер просторот.
    - ОПШТА ЦЕЛ: Обезбедување навремен и координиран одговор на сајбер инциденти и кризи.

        - ПОСЕБНА ЦЕЛ 1. Навремена идентификација, пријавување и соодветен одговор на напади и значајни инциденти поврзани со сајбер просторот
        - ПОСЕБНА ЦЕЛ 2. Навремено и соодветно справување со инциденти со голем опфат и кризи
        - ПОСЕБНА ЦЕЛ 3. Навремено и соодветно справување со сајбер криминал.
- ПРИОРИТЕТНА ОБЛАСТ 5: Национална и меѓународна соработка.
    - ОПШТА ЦЕЛ: Јакнење на националните капацитети и градење доверба во сајбер просторот.
        - ПОСЕБНА ЦЕЛ 1. Соработка на полето на сајбер безбедноста на национално, регионално и меѓународно ниво
        - ПОСЕБНА ЦЕЛ 2. Одговорно однесување на државата и мерки за градење доверба во сајбер просторот

4.3. Резиме на политиките и клучните правци на делување за остварување на општите и посебните цели

Стратегијата за сајбер безбедност 2025 - 2028 годинана Република Северна Македонија поставува пет приоритетни области за градење отпорен и сигурен сајбер простор. Главните политички насоки вклучуваат зајакнување на националните капацитети преку формирање структури за управување, како што се Секторот за сајбер безбедност и тимови за одговор на инциденти (CSIRT); обезбедување безбедност и отпорност на критичната инфраструктура преку управување со ризици и јавно-приватна соработка; унапредување на свесноста и образованието за сајбер заканите; минимизирање на влијанието на сајбер инциденти преку навремена идентификација, координиран одговор и управување со кризи; и зајакнување на националната и меѓународната соработка со НАТО, ЕУ и други партнери за промоција на доверливост и заштита во дигиталниот простор. Овие насоки се реализираат преку мерки како развој на рамка за управување со ризици, воведување механизми за рано предупредување, зајакнување на законодавната рамка и промоција на култура на безбедност во општеството

5. Приоритетна област 1: Силни национални капацитети за сајбер безбедност

Општа цел: Обезбедување на отпорен и сигурен национален сајбер простор.

Во процесот на динамична дигитална трансформација од која е дел и македонскиот дигитален екосистем, постоењето сеопфатна национална рамка што гарантира отпорност на сајбер закани е од исклучителна важност. Таа претставува збир на поврзани правила, стандарди, институции, функции, процеси и лица организирани да нè заштитат од сајбер закани, напади и инциденти.

Овие структури и функции ќе работат во тесна соработка со други субјекти во државата, вклучувајќи ги владиниот, јавниот, приватниот и граѓанскиот сектор, академската и истражувачката заедница. Овој обединет напор е од клучно значење за заштитата на чувствителните податоци и воспоставување безбедна дигитална средина.

Владата на Република Северна Македонија ќе развие јасна структура на управување со сајбер безбедноста за да ги подобри способностите за превенција, спречување, откривање, одговор и закрепнување од сајбер закани и инциденти. Крајна цел е да се осигури дека државата е опремена со вистинските политики и способности за подобрување на сајбер безбедноста на сите владини нивоа.

5.1. Посебна цел 1. Јасна и робусна структура за управување со сајбер безбедноста

Република Северна Македонија ќе се посвети на создавање робустен национален систем за сајбер безбедност, преку изградба на Национална рамка за управување со сајбер безбедност (НРУСБ). Владата на Република Северна Македонија има водечка улога во управувањето со сајбер безбедноста на земјата и е главен двигател на користењето мерки и контроли за сајбер заштита, како и гарант за соработка меѓу засегнатите страни во превенција, идентификација, справување и закрепнување од сајбер инциденти и напади. Со цел да се спротивстави на растечките закани за сајбер безбедноста, преку Стратегијата за сајбер безбедност 2025 - 2028 годинаи придружниот Акциски план, Владата на Република Северна Македонија се обврзува дека ќе направи инвестиции со цел да се поттикне отпорноста на сајбер напади и да се промовира растот на дигиталната средина за дејствување.

Стратегијата за сајбер безбедност 2025 - 2028 година вклучува идентификување оперативни организациски структури и функции, сектори со висока критичност и други важни сектори, како и дефинирање суштински и важни субјекти. Во Анекс 6 е даден дијаграм на организациската поставеност на субјекти и функции во Националната рамка за управување со сајбер безбедноста.

5.1.1. Национален совет за безбедност

Националниот совет за безбедност на Република Северна Македонија игра клучна улога во надгледувањето на безбедноста на земјата, вклучувајќи ја и сајбер безбедноста. Безбедносните служби придонесуваат со клучни информации до Советот. Во однос на сајбер безбедноста, тесно соработуваат за идентификување закани, ублажување ризици и стратешки одговор на сајбер инциденти.
Во контекст на Националната рамка за сајбер безбедност, вклучувањето на безбедносните служби е од витално значење за заштита на критичната инфраструктура, како и за стратешки координиран пристап кон отпорноста на државата на идни закани и напади. Овие служби активно ќе учествуваат во размена на информации и координација на одговори на значајни инциденти и кризи во соработка со засегнати страни вклучително МДТ и. МКД – ЦИРТ.

5.1.2. Национален совет за дигитална трансформација на општеството

Со Стратегијата за сајбер безбедност 2025 - 2028 година се предлага Владата на Република Северна Македонија да го интегрира Националниот совет за сајбер безбедност во Националниот совет за дигитална трансформација на општеството (НСДТО). На овој начин ќе се овозможи координација на активностите на Владата на Република Северна Македонија поврзани со сајбер безбедност и дигитална трансформација на општеството.

НСДТО ќе соработува со МДТ при дефинирање нови стратешки насоки и препораки врзани со сајбер безбедноста, ќе ја следи имплементацијата на Стратегијата за сајбер безбедност 2025 - 2028 година и ќе дава мислења на програми и на акциски планови за одговор на инциденти со голем опфат и сајбер кризи.

5.1.3. Национална Единствена точка за контакт

Национална Единствена точка за контакт (Single Point of Contact – SPOC) е функција одговорна за координирање на прашањата поврзани со сајбер безбедност и прекуграничната соработка.

SPOC обезбедува ефикасна прекугранична соработка со релевантните органи на други земји, земји членки на ЕУ, ЕК, ENISA и НАТО; проследува известувања за значајни и големи инциденти со прекугранично влијание до SPOC на други засегнати земји; овозможува непречена меѓусекторска соработка со другите надлежни органи и засегнати страни во државата[xvi]. Улогата на Национална Единствена точка за контакт ќе ја извршува МДТ. SPOC ќе располага со навремени информации и известувања за пријавени инциденти, закани, напади и други настани поврзани со сајбер безбедноста.

5.1.4. Суштински и важни субјекти

За дефинирање суштински и важни субјекти се користи дефиницијата дадена во член 2 од европската Директива (EU) 2022/2555[xvii].

Суштински субјекти

Суштински субјекти се субјекти што спаѓаат во категориите споменати во Анекс I од Директивата NIS2 и ги надминуваат горните граници за средни претпријатија, во согласност со Член 2 од препораката 2003/361/ЕС, и идентификувани како средни субјекти во согласност со член 470 од Законот за трговските друштва[xviii]. Оваа категорија, исто така, вклучува квалификувани даватели на услуги од доверба, регистри на имиња на домени на највисоко ниво, даватели на DNS-услуги, оператори на јавни електронски комуникациски мрежи или јавно достапни електронски комуникациски услуги, кои се квалификуваат како средни претпријатија, субјекти од јавната администрација и кои било други субјекти идентификувани како суштински субјекти. Субјектите идентификувани како критични субјекти според Директивата (ЕУ) 2022/2557, исто така, се сметаат за суштински субјекти[xix].

Важни субјекти

Важни субјекти се субјектите што не се идентификувани како суштински субјекти, но се наведени во Анекс I или II од Директивата NIS2[xx].

Обврски за суштинските и за важните субјекти

- да ја осигуруваат безбедноста на мрежата, на информациските системи и на податоците што ги користат во своите активности[xxi];
- да усвојат широк опсег основни мерки и контроли за сајбер безбедност какви што се начела на нулта доверба, ажурирања на софтвер, конфигурација на уреди, сегментација на мрежата, управување со податоците и нивно безбедно складирање, управување со идентитет и пристап или свесност за корисниците;
- да организираат обука за нивниот кадар и да ја подигнат свеста за сајбер заканите, за фишингот или за техниките за социјално инженерство[xxii];
- да ги оценат сопствените способности за сајбер безбедност и, онаму каде што е соодветно, да продолжат со интеграција на технологии за подобрување на сајбер безбедноста, какви што се вештачката интелигенција или системите за машинско учење[xxiii];
- да ги проценат и да ги земат предвид севкупниот квалитет и отпорноста на производите и на услугите, мерките за управување со ризикот по сајбер безбедноста вградени во нив и практиките за сајбер безбедност на нивните добавувачи и даватели на услуги, вклучувајќи ги нивните безбедни процедури за развој[xxiv];
- да подложат на административни казни доколку ги прекршат или не ги спроведат пропишаните обврски[xxv].

5.1.5. Тимови за одговор на компјутерски безбедносни инциденти

Државата ќе обезбеди CSIRT (Computer Security Incident Response Team) тимовите за одговор на компјутерски безбедносни инциденти да располагаат со инфраструктура за споделување и обработка на информации, како и со добро обучен и доверлив стручен кадар[xxvi].

CSIRT тимовите се задолжени за следење и анализа на сајбер закани, обезбедување рани предупредувања и споделување информации, одговор на инциденти, форензичка анализа и процена на ризици, и соработка со други CSIRT тимови, на национално и на меѓународно ниво[xxvii].

Владиниот CSIRT ќе има активности поврзани со надзор и заштита на системите и на услугите на Владата на Република Северна Македонија и одговор и координација при справување со инциденти кај овие системи и мрежи и кај субјектите од јавниот сектор. Улогата на Владин CSIRT ќе ја извршува МДТ.

Националниот CSIRT има активности за координација на работата на секторските CSIRT-ови. Во Република Северна Македонија, од 2016 година, улогата на Национален CSIRT ја извршува Националниот центар за одговор на компјутерски инциденти МКД - ЦИРТ, формиран како посебна организациска единица во склоп на Агенцијата за електронски комуникации.

Соработка помеѓу Националниот CSIRT и секторските, организациските, воениот и други CSIRT-ови, вклучува размена на информации за сајбер инциденти и закани, национална координација, координација на одговори на меѓународни инциденти и воспоставување сигурни и ефикасни протоколи за размена на информации со CSIRT во земјата и надвор[xxviii].

Националниот CSIRT ќе има активности поврзани со надзор и заштита на системите и на услугите на суштинските и важни субјекти од секторите со висока критичност во кои не се поставени секторски надлежни авторитети. Активностите вклучуваат евиденција на пријавени инциденти, одговор и координација при справување со инциденти кај овие системи и мрежи, како и размена на информации и координација на активности со Владин CSIRT и надлежни органи од другите сектори со висока критичност.

Надлежностите и соработката на Националниот и на Владиниот CSIRT ќе се уредат со ново законско решение за сајбер безбедност и со измени и усогласувања на постојната ЕУ и НАТО легислатива и добра практика.

5.1.6. Надлежни органи

Надлежните органи се субјекти што имаат овластувања за сајбер безбедност, вклучувајќи пропишување стандарди, мерки и контроли, супервизија на усогласеност, и одговор на инциденти. Тие вршат надзор над суштинските и важни субјекти, спроведуваат инспекции и проверки, издаваат упатства и соработуваат за зголемување на сајбер отпорноста и координација на одговори по инциденти. Важна е и меѓународната соработка, особено кога суштински и важни субјекти обезбедуваат услуги и во други земји, како и соработката со органите за заштита на лични податоци. [xxix]

Национален надлежен орган за сајбер безбедност во државата е МДТ. Воспоставувањето и работата на Националниот надлежен орган и на секторските надлежни органи ќе се уреди со ново законско решение за сајбер безбедност и со усогласување на постојните секторски законски решенија, со транспонирање на обврските и на надлежностите за надлежни органи

(competent authorities) од Директивата (EU) 2022/2555. При изработката на новото законско решение за сајбер безбедност и определувањето на секторските надлежни органи, ќе се земе предвид зрелоста на критичните сектори според постојните законски рамки, воспоставените обврски, мерки и контроли, како и финансиските импликации, за да се обезбеди континуитет и напредок на постојните функции и соработка. Идентификувани секторски надлежни органи се Народната банка на Република Северна Македонија за секторот „Банкарство“, Регулаторната комисија за енергетика за секторот „Енергетика“ и Агенцијата за електронски комуникации за потсекторите „Даватели на јавни електронски комуникациски мрежи“ и „Даватели на јавно достапни електронски комуникациски услуги“ од секторот „Дигитална инфраструктура“.

Секторските надлежни органи соработуваат, разменуваат информации и ги координираат своите активности со Националниот надлежен орган (МДТ) и ги проследуваат пријавените инциденти до MKD-CIRT.

5.1.7. Управување со инциденти со голем опфат и кризи

Координација и справување со сајбер криза и инциденти по сајбер безбедност со голем опфат врши МДТ и Владиниот CSIRT, преку одговор на инцидентите во соработка со Националниот CSIRT, Центарот за управување со кризи, Националниот совет за дигитална трансформација на општеството, Министерството за надворешни работи, Министерството за одбрана, безбедносните структури, суштинските и важните субјекти и другите засегнати страни.

Надлежностите на МДТ ќе вклучуваат усвојување рамковна политика за координација и споделување информации за ризици и инциденти, имплементација и тестирање на План за координиран одговор на големи прекугранични кризи, и идентификација и ажурирање на ресурси потребни за брз и ефикасен одговор на криза. Управувањето со инциденти со голем опфат и кризи, ќе се уреди со новото законско решение за сајбер безбедност и преку усогласување со постојната легислатива за управување со кризи.

5.1.8. Градење професионални капацитети за сајбер безбедност

Изградбата на стручна работна сила за сајбер безбедност во јавниот сектор е од суштинско значење за заштита на националната инфраструктура од растечките сајбер закани. Брзата дигитализација на критичните услуги и континуираната еволуција на сајбер нападите наложува државата да преземе активности насочени кон зајакнување на капацитетите за сајбер безбедност. Потребно е воведување или подобрување на постојните заложби за континуиран професионален развој на професионалците, поддршка за специјализирани програми за обука и поттикнување соработки со академските институции.

5.1.9. Клучни мерки

Клучните мерки за остварување на оваа цел ќе бидат:

- Креирање јасна организациска шема за структурата на сајбер безбедност на Владата на Република Северна Македонија;
- Воспоставување јасни владини политики за комуникација и соработка, со дефинирани улоги и надлежности поврзани со сајбер безбедноста;
- Ново законско решение за сајбер безбедност што ќе ја дефинира Националната рамка за сајбер безбедност;

- Интеграција на Националниот совет за сајбер безбедност во Националниот совет за дигитална трансформација;
- Формализирање на постојните работни групи и воспоставување нови, поврзани со заштита во сајбер просторот, заштита на мрежните и на информациските системи, и сајбер безбедноста како основа за успешна дигитална трансформација;
- Развивање специјализирани програми за обука и образование за сајбер безбедност за вработените во јавниот сектор;
- Зајакнување на јавно-приватните партнерства, соработката со стопанските комори, јавниот, граѓанскиот и приватниот сектор, академската и истражувачка заедница, и споделување на знаење во сајбер безбедноста;
- Практични работилници за вработените во јавниот сектор, фокусирани на одговор на инциденти и заштита на инфраструктурата;
- Специфични патеки за кариера и програми за развој на кариера за работни места во сајбер безбедност во јавен сектор;
- Развивање стимуланси за вработените што се преквалификуваат за работни места за сајбер безбедност во јавен сектор;
- Меѓународна соработка за развој на таленти во сајбер безбедноста;
- Рамковна политика за координација и споделување информации за ризици и инциденти;
- План за координиран одговор на инциденти со голем опфат и кризи;
- Идентификација и ажурирање на ресурси потребни за брз и ефикасен одговор на кризи.

5.2. Посебна цел 2: Формирање на Сектор за сајбер безбедност во Министерство за дигитална трансформација

За да биде во чекор со тековните и идните сајбер закани, Владата на Република Северна Македонија постојано ќе ги унапредува своите технички и оперативни способности за откривање и реагирање на инцидентите на сајбер безбедноста. Ќе се формираат оперативни единици во рамките на МДТ опремени со соодветни човечки, технички и финансиски ресурси. Овие единици ефективно ќе соработуваат со националните тела, приватната индустрија, истражувачките заедници и со меѓународните организации[xxx].

За таа цел во МДТ ќе се формира Сектор за сајбер безбедност – ССБ со оперативни единици на ниво на одделенија. Овој сектор ќе биде одговорен за безбедносен надзор над владини мрежи, системи и услуги како и за примена на превентивни и реактивни мерки при безбедносни инциденти кај нив. Секторот ќе обезбеди поддршка на лице место за сериозни инциденти по сајбер безбедноста кај институции од јавниот сектор, ќе открива и ќе оценува инциденти што ги засегаат владините мрежи, системи и услуги, и ќе ја зајакне стратегиската определба на државата за безбеден сајбер простор[xxxi].

ССБ при МДТ со оперативни капацитети ќе ги обединува следните функции:

- Национален орган одговорен за сајбер безбедност;
- Национална Единствена точка на контакт за сајбер безбедност (SPOC);
- Владин тим за одговор на компјутерски безбедносни инциденти – Владин CSIRT;
- Национален орган за координација и управување со компјутерски безбедносни инциденти со голем опфат и кризи;
- Подготовка на стратешки документи и политики;
- Следење на имплементацијата на Стратегијата за сајбер безбедност и Акцискиот план, како и други стратешки документи;

- Анализи за потреби за стратешко планирање во областа на националната сајбер безбедност;
- Пропишување стандарди, мерки и контроли за сајбер безбедност за владините мрежи, системи и услуги, и за јавниот сектор;
- Надзор над безбедноста на владините мрежи, системи и услуги;
- Супервизија на усогласеност на институциите од јавниот сектор со пропишаните стандарди, мерки и контроли;
- Соработка со Националниот CSIRT и со други владини институции и организации во државата;
- Меѓународна соработка и градење стратешки партнерства;
- Соработка со организациите и мрежите на Европската Унија одговорни за управување со инциденти со голем опфат и кризи (EU-CyCLONe).

За работата на ССБ при МДТ, неопходно е да се обезбедат човечки, технички и финансиски ресурси. Со тоа ќе се овозможи ССБ да одговори на зголемената потреба за професионална поддршка на лице место за владините критични ИКТ-системи и услуги, како и за институциите од јавниот сектор[xxxii].

Преку ССБ ќе се овозможи зајакнување на стратешкиот капацитет на Република Северна Македонија и ќе се обезбеди позитивно влијание врз напредокот кон безбеден сајбер простор, овозможувајќи ѝ на државата да открие, да реагира и да се брани од малициозни сајбер напади[xxxiii].

5.2.1. Клучни мерки

- Формирање Сектор за сајбер безбедност при МДТ како Национален орган одговорен за сајбер безбедност и Единствена точка за контакт за сајбер безбедност (SPOC);
- Воспоставување владин безбедносен оперативен центар (Security Operations Center – SOC), за превентивен надзор и грижа за сајбер безбедноста на мрежи, системи и услуги на МДТ и на Владата на Република Северна Македонија;
- Меѓународна соработка и градење стратешки партнерства;
- Воспоставување Национален орган за координација и управување со компјутерски безбедносни инциденти со голем опсег и кризи;
- Подготовка на стратешки документи и политики и следење на имплементацијата на Стратегијата за сајбер безбедности Акцискиот план, и други стратешки документи;
- Пропишување стандарди, мерки и контроли за сајбер безбедност за владините мрежи, системи и услуги, и за јавниот сектор;
- Супервизија на усогласеност на институциите од јавниот сектор со пропишаните стандарди, мерки и контроли.

5.3. Посебна цел 3. Зголемени капацитети за одбранбени операции во сајбер просторот

За ефикасно справување со ризиците во сајбер просторот, Република Северна Македонија ќе гради капацитети за сајбер одбрана според највисоките стандарди, како составен дел од Националната рамка за сајбер безбедност. Развојот на капацитетите за сајбер одбрана во Армијата се од стратешко значење за целокупната национална одбрана на земјата. Армијата ќе

развие воен тим за одговор на компјутерски безбедносни инциденти и можности за распоредување на сајбер операции.

5.3.1. Клучни мерки

- Унапредување на капацитетите за воени сајбер операции преку развој на сеопфатна стратегија за подобрување на капацитетите за сајбер операции на војската.
- Формирање воен тим за одговор на компјутерски безбедносни инциденти.
- Развој на способности за сајбер одбрана за национални и воени потреби преку создавање цврста рамка за распоредување на способности за сајбер одбрана за заштита на националната безбедност и на воените операции.

6. Приоритетна област 2: Безбедност и отпорност на суштински и важни субјекти, мрежи и информациски и комуникациски системи

Општа цел: Обезбедување на безбедноста, доверливоста и отпорноста на критичните мрежи, информациски системи и суштинските и важни субјекти.

Достапноста, доверливоста и интегритетот на податоците и на услугите што ги обезбедуваат суштинските и важните субјекти, придонесуваат за нормално функционирање на општеството и на државата. Јавниот и приватниот сектор, преку заедничко користење човечки, технички и организациски ресурси, заедно ќе ја остварат безбедноста и отпорноста на критичната информациска инфраструктура. Заштитата на мрежите и на информациските системи кај суштинските и важните субјекти (оператори на критична инфраструктура) и заштитата на индустриски контролни системи е од голема важност, имајќи предвид дека тие субјекти во најголем дел ја поседуваат мрежната и информациската инфраструктура што е од значење за државата. Дополнително од важност е заштитата на ИКТ-услугите и системите што ги користи Владата на Република Северна Македонија, јавниот и приватниот сектор.

За да се постигне безбедна и отпорна мрежна и информациска инфраструктура и заштита на податоци, потребно е редовно спроведување безбедносни мерки, со фокус на превенција, откривање и одговор на инциденти, развивање нови безбедносни решенија, зајакнување на координацијата и соодветно приспособување на законските обврски.

6.1. Посебна цел 1. Управување и следење ризици и закани

Идентификацијата и управувањето со националните сајбер ризици имаат за цел да приоритизираат и да развијат соодветни процедури за справување со нив, со ставање посебен фокус на ризиците поврзани со производители и добавувачи на ИКТ-опрема и услуги, како и на тие поврзани со синџир за снабдување.

Соработката меѓу јавниот и приватниот сектор и секторите со висока критичност ќе води кон подобро разбирање, приоритизирање и управување со сајбер ризиците и заканите што опфаќаат еден или повеќе критични сектори.

ќе се воведе континуирана процена и управување со ризиците и нивно ублажување кај јавниот сектор и суштинските и важни субјекти во државата, преку едуциран стручен кадар и преку примена на меѓународни стандарди за управување со сајбер ризици.

Поддршката на приватниот сектор во процена и управување со сајбер ризиците ќе се обезбеди преку давање упатства за процена на сајбер ризици засновани на меѓународни стандарди и едукација на правните лица преку соодветни обуки.

Ќе се донесе Национална рамка за процена на ризици поврзани со сајбер безбедност што понатаму ќе се користи во владиниот и во јавниот сектор и кај суштинските и важни субјекти.

Воспоставување Регистар на идентификувани информациски основни средства од големо значење за државата што континуирано ќе се ажурира и ќе се врши оцена на ризиците поврзани со идентификуваните ранливости, закани и ризици кај овие средства, кај мрежите и ИКТ-системите во јавниот сектор и кај суштинските и важни субјекти. Неопходно е овие регистри периодично да се ажурираат, во согласност со актуелните ранливости и закани. Размената на информации за ранливости, закани, инциденти и ризици ќе се подигне на повисоко ниво преку Мрежата за споделување информации на Националниот CSIRT тим и Националниот орган одговорен за сајбер безбедност. За таа цел ќе се воспостави политика за управување со ранливости, што опфаќа промовирање и олеснување на координирано откривање ранливости[1].

Неопходно е суштинските и важните субјекти да преземаат соодветни и пропорционални технички, оперативни и организациски мерки за да управуваат со ризиците поврзани со безбедноста на мрежните и на информациските системи што тие субјекти ги користат за своето работење или за обезбедување на нивните услуги, како и да го спречат или да го минимизираат влијанието на инцидентите врз корисниците на нивните услуги и врз другите директно или посредно поврзани услуги. Притоа, овие мерки треба да обезбедат ниво на безбедност на мрежните и на информациските системи пропорционално на ризиците што се поставуваат. При процена на пропорционалноста на тие мерки, соодветно ќе се зема предвид степенот на изложеност на ентитетот на ризици, големината на ентитетот и веројатноста за појава на инциденти и нивната сериозност, вклучувајќи го нивното општествено и економско влијание.

Ќе се воведе Политика за процена на безбедносниот ризик на критичните синџири за снабдување, преку процена на безбедносниот ризик на специфичните критични ИКТ-услуги, ИКТ-системи или синџири за снабдување со ИКТ-решенија, земајќи ги предвид техничките и нетехничките фактори на ризик. Притоа, во проценатa ќе се земат предвид и проценитe направени на ниво на Европската Унија и во земји членки на ЕУ.

Националниот надлежен орган во соработка со другите надлежни органи ќе дефинира и ќе ажурира оперативни и организациски мерки за управување со ризиците поврзани со безбедноста на мрежните и на информациските системи кај суштинските и важни субјекти, што тие субјекти ги користат за своето работење или за обезбедување на нивните услуги.

Националниот надлежен орган во соработка со други надлежни органи ќе врши надзор над суштинските и важни субјекти во делот на имплементација на пропишаните мерки и контроли и проценатa на ризиците.

Законска обврска за суштински и важни субјекти да преземаат соодветни и пропорционални технички, оперативни и организациски мерки за да управуваат со ризиците поврзани со безбедноста на мрежните и на информациските системи.

6.1.1. Клучни мерки

- Национална рамка за процена на ризици поврзани со сајбер безбедност;
- Оперативни и организациски мерки за управување со ризиците поврзани со безбедноста на мрежните и на информациските системи кај суштинските и важни субјекти;
- Надзор над суштинските и важни субјекти во делот на имплементација на пропишаните мерки и контроли и проценатa на ризиците;
- Управување со ранливости, што опфаќа промовирање и олеснување на координирано откривање на ранливоста.

6.2. Посебна цел 2: Безбедни и отпорни суштински и важни субјекти

Одговорноста за обезбедување на безбедноста на податоците, мрежите, и информациските системи, во ИТ (Информациски Технологии) и ОТ (Оперативни Технологии) системите, вклучувајќи ги и контролните системи, во голема мера е кај суштинските и важни субјекти. Со Стратегијата за сајбер безбедност 2025 - 2028 година се промовира култура на управување со ризик, што вклучува процени на ризик и имплементација на мерки за управување со ризик по сајбер безбедност, соодветни на заканите со кои се соочуваме. Императив е да се воспостават робусни мерки за сајбер безбедност засновани на процена на ризици во идентификуваните критични сектори во државата. Дополнително, се препорачува нивна имплементација и од страна на јавниот, приватниот и граѓанскиот сектор[xxxiv].

Соработката помеѓу јавниот и приватниот сектор, суштинските и важните субјекти, во делот на рано препознавање на заканите и споделување информации, е клучна за заштита на критичната инфраструктура и брзата реакција на сајбер заканите и инцидентите[xxxv]. Соработката и размената на информации придонесуваат за рано откривање малициозни активности, овозможувајќи проактивен пристап и побрз одговор на потенцијалните сајбер закани[xxxvi].

Воспоставувањето и развојот на тимови за одговор на компјутерски безбедносни инциденти со национални, владини и секторски надлежности (CSIRT) кај надлежните органи, како и воспоставување центри за активности поврзани со безбедност (Security Operations Center – SOC) кај суштинските и важните субјекти, се од витално значење за создавање сеопфатен пристап кон отпорноста на закани и ранливости[xxxvii].

Операторите како суштински и важни субјекти во секторите со висока критичност ќе добијат поддршка во заштитата на нивната инфраструктура, придонесувајќи за развој на безбедносни мерки за спротивставување и постигнување отпорност на напади врз информациските и комуникациските системи[xxxviii].

Суштинските и важните субјекти ќе применуваат и ќе спроведуваат политики и мерки за управување со ризици за сајбер безбедност[xxxix], како дел од Национална рамка за управување со ризици поврзани со сајбер безбедноста, со Методологија за процена на ризиците.

Идентификацијата на суштинските и на важните субјекти ќе се уреди со ново законско решение за сајбер безбедност и со усогласување на постојните секторски законски решенија, со транспонирање на обврските и на надлежностите за надлежни органи од Директивата (EU) 2022/2555.

6.2.1. Клучни мерки:

- Изработка и усвојување на Национална рамка за управување со ризици поврзани со сајбер безбедноста со методологија за процена на ризиците;
- Подобрување на отпорноста на суштински и важни субјекти;
- Поддршка на субјектите во справување со сајбер напади и инциденти.

6.3. Посебна цел 3. Подобрена безбедност на националните мрежи и информациски системи

Мрежите и информациските системи од национално значење се оние што обезбедуваат услуги што се од суштинско значење за одржување на критичните општествени и економски активности. Прекинот на овие системи би имал значително влијание врз јавната безбедност, јавното здравје или економијата, а ги вклучуваат сектори со висока критичност.

Неопходно е обезбедување ефикасен систем за заштита и сертификација на националните мрежи и информациски системи низ кои се процесираат класифицирани информации, за континуирано унапредување на заштитата од сајбер напади и сајбер шпионажа.

На државно ниво ќе се донесат обврзувачки Минимални технички и организациски мерки за сајбер безбедност, за оператори во секторите со висока критичност. Тие ќе се усогласат со постојните ISO и NIST стандарди, како и со Национална рамка за управување со ризици поврзани со сајбер безбедност, која ќе ги вклучи и националните мрежи и информациски системи.

Овие мерки континуирано ќе се приспособуваат во согласност со актуелното ниво на сајбер заканите и брзиот развој на технологијата. Ќе се воведе задолжителна проверка на усогласеноста кај суштинските и важните субјекти (операторите) со утврдените Минимални технички и организациски мерки за сајбер безбедност.

6.3.1. Клучни мерки

- Дефинирање минимален сет технолошки и организациски мерки за сајбер безбедност;
- Поддршка при имплементација и надзор над усогласеност на минималниот сет на технолошки и организациски мерки за сајбер безбедност;
- Континуирано подобрување на безбедносната акредитација за комуникациско-информациските системи низ кои се процесираат класифицирани информации, со цел да се обезбеди највисок степен на заштита од сајбер напади и шпионажа.

6.4. Посебна цел 4. Препораки за употреба на безбедносната технологија во општеството

Владата на Република Северна Македонија се залага за создавање безбедна дигитална средина преку стратешка поддршка и промоција за користење дигитални безбедносни технологии, вештачка интелигенција, квантни технологии и електронски комуникации. Овие технологии, кога ефективно се имплементираат и управуваат, можат да обезбедат значителна заштита од тековни и идни сајбер закани. За таа цел, со Стратегијата за сајбер безбедност 2025 - 2028 година се предвидува следење и поддршка на нови безбедносни технологии, соработка помеѓу академскиот, јавниот сектор и CSIRT тимовите за ефикасни безбедносни процени. Со Стратегијата за сајбер безбедност 2025 - 2028 година се воведува промоција на сертифицирани технологии особено кај суштинските и важни субјекти при користење ИКТ-производи, услуги и

процеси, кои се сертифицирани според европските шеми за сертификација на сајбер безбедност – во согласност со Регулативата (ЕУ) 2019/881. Дополнително, се вклучуваат сајбер безбедносни барања во јавните набавки и воспоставување регистри на безбедни и високоризични технологии.

6.4.1. Клучни мерки

- Политика за вклучување и спецификација на барањата поврзани со сајбер безбедноста за ИКТ-решенија и ИКТ-услуги во јавните набавки, вклучително и во врска со сертификацијата за сајбер безбедноста, шифрирањето и употребата на производи за сајбер безбедноста со отворен код;
- Регистар на безбедни нови технологии;
- Регистар на технологии што претставуваат висок безбедносен ризик;
- Постојана меѓуресорна работна група при НСДТО задолжена за следење нови технологии, оценка на нивна безбедност и издавање препораки за користење.

6.5. Посебна цел 5. Партнерство и соработка помеѓу државните и приватните капацитети

Стратегијата за сајбер безбедност 2025 - 2028 годинаистакнува дека јавно-приватните партнерства (ЈПП), соработката со стопанските комори и аутсорсингот се клучни модели за зајакнување на сајбер безбедноста и градење отпорно општество. Овие форми на соработка овозможуваат комбинирање ресурси, експертиза и иновации од различни сектори, што води кон поефикасна и брза реакција на сајбер заканите.

ЈПП играат важна улога преку обединување на капацитетите на Владата на Република Северна Македонија и на приватниот сектор за развој на заеднички инфраструктури и системи за заштита. Од друга страна, аутсорсингот овозможува користење надворешна експертиза и технички решенија, кои можат да ги подобрат способностите за одбрана од сајбер напади. Соработката со стопанските комори, пак, им дава поддршка на микро, малите и средните претпријатија, кои се витални за македонската економија, во развојот на сајбер безбедносни стратегии.

Сите овие форми на соработка се неопходни за изградба на доверлива и безбедна дигитална инфраструктура, која ќе го штити општеството од растечките сајбер закани.

6.5.1. Клучни мерки

- Мултисекторска работна група: Воспоставување постојана работна група под водство на МДТ, која ќе ги обедини јавниот и приватниот сектор, стопанските комори и аутсорсинг провајдерите за размена на информации и заеднички иницијативи во сајбер безбедноста.

7. Приоритетна област 3: Општество отпорно на сајбер закани

Општа цел: Создавање свесно и отпорно општество.

Дигиталната трансформација со себе носи придобивки, но и безбедносни предизвици на кои мора да се реагира со подготвеност. Зголемената употреба на технологијата, како и непознавањето на ризиците во сајбер просторот, ја нагласува потребата од преземање

соодветни мерки и процедури, кои ќе придонесат општеството да биде отпорно на сајбер ризиците. Од исклучителна важност е создавање граѓанска култура на отпорност кон сајбер заканите.

Оваа приоритетна област вклучува имплементација на програми и активности во образовниот систем за зголемување на свесноста и стекнувањето со основно познавање за сајбер безбедноста. Особено е важно имплементација на соодветни програми и активности за зголемување на свесноста за сајбер безбедност кај вработените во јавниот и во приватниот сектор, како и кај целокупното население. Од голема важност за остварувањето на оваа цел е развојот и спроведувањето на програми во високото образование за едукација и обука на сајбер професионалци, кои ќе можат да се справат со софистицирани и комплексни напади во сајбер просторот.

7.1. Посебна цел 1. Зголемување на свесноста за сајбер безбедноста и дезинформации во сајбер просторот

Свесноста за ризиците што постојат во сајбер просторот за граѓаните, како и за вработените во јавниот и во приватниот сектор, е основен предуслов за поефикасна заштита од сајбер напади и дезинформации во сајбер просторот. Најголем дел од корисниците не ги познаваат или соодветно не ги практикуваат основните безбедносни правила. Преку спроведување на Планот за подобрување на општото ниво на свесност за сајбер безбедноста кај граѓаните, ќе се обезбеди системски пристап кон подобрена заштита на граѓаните.

Суштинските и важни субјекти треба да усвојат широк опсег на основни практики за сајбер хигиена, какви што се начела на нулта доверба, навремено ажурирање на софтвер, конфигурација на уреди, сегментација на мрежа, управување со идентитетот и пристапот на корисниците. Субјектите треба да организираат обуки за вработените и да ја подигнат свесноста за сајбер заканите, за фишинг и за други техники на социјален инженеринг. Суштинските и важни субјекти треба континуирано да прават процена на сопствените способности за сајбер безбедност. Онаму каде што е соодветно, субјектите треба да продолжат со интеграција на технологии за подобрување на сајбер безбедноста, какви што се вештачката интелигенција или системите за машинско учење.

Наставните програми во основното, средното и високото образование треба да се надградат и да се ажурираат со цел подигнување на свеста и едукација за сајбер безбедност, критично размислување и заштита од дезинформации во сајбер просторот. Потребно е да се усовршат постојните и да се развиваат нови наставни програми во сите циклуси на студии на универзитетите во Република Северна Македонија, за да ги задоволат во целост потребите на државата за едуцирање и обука на професионалци во областа на сајбер безбедноста, како и за учество во истражувачки проекти и поддршка на истражувачки капацитети и бизнис-иновации во оваа област.

Формирањето национален институт и други институти/центри за едукација и истражување за сајбер безбедност и дигитална форензика, со цел едукација, доедукација и обука на сајбер професионалци на владино ниво, на јавната администрација и на други чинители на кои им е потребен ваков вид образование и обука, е исто така од круцијално значење за исполнување на оваа цел.

7.1.1. Клучни мерки

- План за подобрување на општото ниво на свесност за сајбер безбедноста што ќе ги вклучи најмалку неопходните мерки;
- План за подобрување на едукацијата во основно и средно образование за критично размислување и заштита од дезинформации во сајбер просторот;

- Подигнување на свеста и едукација за сајбер безбедност во основното и средното образование;
- Подигнување на свеста и едукација за сајбер безбедност во високото образование;
- Подигнување на свеста и едукација за сајбер безбедност на вработените во јавниот и во приватниот сектор;
- Задолжителна обука за сајбер безбедност за сите вработени во јавен сектор;

- Континуирано подобрување на постојните студиски програми од сите циклуси на високо образование поврзани со сајбер безбедноста, креирање нови и придружни активности поврзани со сајбер безбедност и студентите;
- Подигнување на свеста и едукација за сајбер безбедност за граѓаните;

- Координација на активности за развој и реализација на програми за едукација и обука на сајбер професионалци
- Развој и доопремување на Институтот за сајбер безбедност и дигитална форензика;
- Развој и доопремување на постојните институти/центри/лаборатории за сајбер безбедност и дигитална форензика на релевантни Македонски универзитети;
- Континуирано подобрување на постоечките студиски програми од сите циклуси на високото образование поврзани со сајбер безбедноста, креирање на нови и пропратни активности поврзани со сајбер безбедност и студентите.

7.2. Посебна цел 2. Заштита на деца и млади на интернет

Стратегијата за сајбер безбедност 2025 - 2028 година вклучува посебен фокус на заштита на деца и млади на интернет.

МДТ во соработка со МСПДМ, МОН, МВР, МНРНТ, МКД ЦИРТ и други засегнати страни ќе иницира развој на План за заштита на деца и млади на интернет.
Република Северна Македонија ќе разменува информации и добри практики со други држави преку меѓународни иницијативи и ќе промовира примена на меѓународните стандарди и рамки за заштита на деца на интернет во државата.

Подобрување на постојните закони за сајбер безбедност за да се вклучат специфични одредби за заштита на децата од онлајн злоупотреба, малтретирање и експлоатација.

Воспоставување партнерства со технолошките компании и интернет-провајдерите за создавање алатки што ќе ги заштитат децата од штетна содржина, сајбер булинг и сексуална експлоатација.

Формирање центар посветен на заштита на децата на интернет, кој ќе ги обединува експертите од јавниот и од приватниот сектор, академијата и невладини организации. Овој центар ќе биде одговорен за следење на онлајн заканите и давање совети и поддршка на децата и на родителите. Проектот за формирање Национален центар за побезбеден интернет MKSafeNet одговара на повикот „Забрзување на најдобрата употреба на технологии (DIGITAL-2023-DEPLOY-04)“ со поддршка на националните центри за побезбеден интернет во земјите членки на ЕУ и

асоцираните членки. Република Северна Македонија сè уште нема воспоставен Национален центар за побезбеден интернет (CIC). Преку овој проект ќе се создаде основна инфраструктура за воведување сеопфатен CIC, подобрувајќи ги постојните иницијативи од јавниот и од приватниот сектор. Целта е да се подобрат услугите, да се олесни пристапот до соодветна содржина и да се зголеми свесноста за онлајн ризици и можностите за пријавување. MKSafeNet се сосредоточува на зајакнување на националните капацитети за поддршка на децата, на младите, на родителите и на наставниците за побезбедно дигитално искуство, како и на обезбедување поддршка за жртвите на сајбер малтретирање и за ранливите групи.

7.2.1. Клучни мерки:

- План за заштита на деца на интернет.
- Создавање јасни правни механизми за пријавување и следење онлајн криминал против деца.
- Иницијатива на МДТ со интернет-провајдерите за промоција на филтри за блокирање штетна содржина за децата.
- Промоција и воведување алатки за родителска контрола и безбедно пребарување на интернет за помладите корисници.
- Национален центар за побезбеден интернет MKSafeNet.

8. Приоритетна област 4: Минимизирање на влијанието на инцидентите во сајбер просторот

Општа цел: Обезбедување навремен и координиран одговор на сајбер инциденти и кризи.

Сајбер нападите и инцидентите се случуваат секојдневно и со сè поголем интензитет. За да се намали штетата и да се обезбеди поддршка за жртвите, потребно е да се преземат мерки за превенција, спречување, идентификација и ублажување на инцидентите. Важно е да се имплементираат технички и организациски мерки за управување со ризиците, како и задолжително пријавување значајни инциденти. Подобрувањето на координацијата за управување со инциденти и обезбедувањето поддршка за жртвите, ќе овозможи ефикасно справување со заканите.

8.1. Посебна цел 1. Навремена идентификација, пријавување и соодветен одговор на напади и значајни инциденти поврзани со сајбер просторот

8.1.1. Идентификација на инциденти

Идентификацијата на инциденти поврзани со сајбер просторот е критична за заштитата на мрежите и на информациските системи од национално значење, особено оние што припаѓаат на суштински и важни субјекти. Овие мрежи и системи се од витално значење за одржување на националната безбедност и економската стабилност, па затоа нивната заштита од сајбер напади мора да биде приоритет.

Воведувањето континуирано следење и мониторинг на овие системи е клучно за рано откривање сајбер инциденти, какви што се злонамерни упади, напади од типот DDoS или кражба на чувствителни податоци. Мрежните сензори и системите за откривање упади (IDS) играат важна улога во идентификацијата на сомнителни активности, додека соработката со националниот и со владиниот тим за одговор на компјутерски инциденти (CSIRTs) ќе овозможи брз одговор и координација.

8.1.2. Пријавување сајбер инциденти и сајбер криминал

Едноставното пријавување сајбер инциденти и пријава на сајбер криминал, стручноста и способноста на државните органи одговорни за справување со сајбер напади и инциденти што ќе овозможат соодветна и навремена поддршка, ќе помогнат во зголемување на бројот на пријави на инциденти и подобрена видливост за тековни сајбер настани со кои се соочува државата. Пријавените информации ќе се користат за анализи на настанатите инциденти од кои произлегуваат насоки за спречување идни инциденти, ќе помагаат при истраги за компјутерски криминал и ќе овозможат креирање информации од стратешка важност за државата.
Инцидентот ќе се смета за значаен доколку: (а) предизвикал или е способен да предизвика сериозно оперативно нарушување на услугите или финансиски загуби за засегнатото правно лице; и (б) ги погодил или е способен да ги погоди другите физички или правни лица со предизвикување значителна материјална или нематеријална штета.

Идентификуваните суштински и важни субјекти (понатаму „субјекти“) ќе имаат обврска за пријава на значајни инциденти до Националниот CSIRT (MKD-CIRT), како и до секторскиот и Националниот надлежен орган доколку тоа е уредено со законско решение.

Субјектите од јавниот сектор ќе пријавуваат значајни инциденти до Секторот за сајбер безбедност при МДТ (Владин CSIRT). Владиниот CSIRT без одложување ќе ги проследува овие пријави и до Националниот CSIRT. Секторот за сајбер безбедност при МДТ ќе гради капацитети за одговор и помош во справување со овие инциденти.

Воспоставувањето единствена точка за пријава на сајбер инциденти и компјутерски криминал ќе овозможи уште подобра соработка помеѓу Националниот CSIRT, Владиниот CSIRT и Министерството за внатрешни работи. Единствената точка ќе биде дел од Систем за соработка и размена на информации, поддршка при одговор и координација во справување со инцидентите. Честопати сајбер инцидентите преминуваат во сајбер криминал и подобрената соработка ќе овозможи размена на корисни информации меѓу организациите, во насока за ефективно и брзо решавање инциденти и случаи на криминал.

Законското решение за сајбер безбедност со кое ќе се воведе и ќе се регулира задолжителното пријавување инциденти и напади од страна на суштинските и важните субјекти, како и напади на критичните ИКТ-услуги, системи и решенија, владиниот и јавниот сектор, ќе има позитивно влијание во сајбер просторот. На тој начин што ќе се постигне поширока информираност и запознавање со актуелните напади и ризици.

Националната категоризација и класификација за сајбер инциденти и приоритизирање во нивното решавање со одредени улоги и одговорности на учесниците, ќе помогнат во навремен и квалитетен одговор и во координацијата со цел успешно и ефикасно справување со сајбер инциденти и напади.

8.1.3. Одговор на значајни инциденти

Во насока на навремената идентификација и одговор на значајни инциденти, воспоставени и квалитетно опремени, екипирани и оперативни CSIRT тимови и тимови за брз одговор, ќе придонесат за побрза и поефикасна размена на информации за инциденти и брз и квалитетен одговор по настанат инцидент. Овие CSIRT тимови ќе се грижат за безбедноста на критичната инфраструктура во дадениот сектор, со дефиниран мандат, со надлежности и соработка со операторите од засегнатиот сектор, како и соработка и координација со Националниот CSIRT и Владиниот CSIRT.
Ќе се развие Систем за соработка и размена на информации, поддршка при одговор и координација во справување со инцидентите, меѓу Владиниот CSIRT, Националниот CSIRT тим,

секторските и други CSIRT тимови, надлежните органи и други засегнати организации во државата. На тој начин ќе се обезбеди подобрена видливост на негативните настани во сајбер просторот, координација во справување со инцидентите што опфаќаат повеќе сектори, значајни инциденти и сајбер напади што се од национално значење. Системот ќе го воспостави Националниот CSIRT во соработка со Владиниот CSIRT и другите засегнати страни.

Имплементација на механизми за детекција и одговор на сајбер инциденти кај субјектите ќе овозможи детален и навремен увид во моменталната состојба на национално ниво и ќе го намали времето за реакција, постапување и решавање на инцидентите.

Воспоставување Национален тим за брз одговор по настанат сајбер инцидент е од голема важност за државата. Во соработка меѓу МДТ, секторски надлежни органи, Националниот, Владиниот и други CSIRT-тимови, ќе се формира регистар на експерти со специфични високоспецијализирани знаења и вештини, кои ќе бидат повикани и координирани од МДТ во случаи за одговор по сајбер напади и инцидент од голема важност за државата. Регистарот ќе опфати и хардверски и софтверски средства, кои се од важност за навремен одговор по сајбер напади и инциденти, со цел брзо организирање и ефективна и ефикасна координација на одговор по напади и инциденти.

8.1.4. Клучни мерки

- Надзор над мрежите и информациските системи кај суштински и важни субјекти од страна на MKD-CIRT и Владин CSIRT кај владините мрежи и системи;
- Систем за соработка и размена на информации, поддршка при одговор и координација во справување со инцидентите;
- Воспоставување единствена точка за пријава на сајбер инциденти и компјутерски криминал во сајбер просторот и понатамошна соработка меѓу Националниот CSIRT, Владиниот CSIRT и Сектор за компјутерски криминал при Министерството за внатрешни работи и интеграција во системот за соработка и размена на информации;
- Национална категоризација и класификација за сајбер инциденти и напади, и приоритизирање во нивното решавање;
- Поддршка за воспоставување квалитетно опремени, екипирани и оперативни CSIRT тимови при секторските надлежни органи, во секторите со висока критичност и други критични сектори;
- Стандардизирани оперативни процедури, правила и обврски при соработка и размена на информации, поддршка при одговор и координација во справување со инцидентите меѓу Националниот CSIRT тим, Владиниот CSIRT, други CSIRT тимови и другите засегнати страни;
- Механизми за детекција и одговор на сајбер напади и инциденти во организациите – суштински и важни субјекти;
- Тимови за брз одговор на сајбер напади и инциденти од државно значење (Rapid response);
- Национален Регистар на сајбер ресурси.

8.2. Посебна цел 2. Навремено и соодветно справување со инциденти со голем опфат и кризи

Со Стратегијата за сајбер безбедност 2025 - 2028 година се предвидува воспоставување Национална рамка за управување со сајбер кризи, преку идентификација на органите задолжени за координација, одговор и справување со кризи по сајбер безбедноста. Рамката

опфаќа и дефинирање на потребните средства и ресурси за успешно справување со кризи, а ги вклучува и мерките што треба да ги применуваат субјектите.

Редовна проверка и практично тестирање на одговор на инциденти од голем опфат на национално и на меѓународно ниво, вклучувајќи го и политичкиот одговор, онаму каде што е потребно и со вклучување субјекти од приватниот сектор[xl].

Ефективниот одговор на големи инциденти и кризи по сајбер безбедноста на меѓународно ниво бара брза и ефикасна соработка меѓу сите релевантни чинители. Ова се потпира на подготвеноста и на способностите на поединечните земји, како и на координираната заедничка акција[xli].

Навремениот и ефективен одговор на инцидентите се потпира на постоењето на претходно воспоставени и добро извежбани процедури и механизми за соработка, кои јасно ги дефинираат улогите и одговорностите на клучните актери на национално и на меѓународно ниво[xlii].

Планот за координиран одговор се однесува на инциденти по сајбер безбедноста, кои предизвикуваат преголеми нарушувања за да може земјата сама да се справи или кои влијаат врз две или повеќе земји или меѓународни организации. Овие инциденти имаат значително влијание од техничко или политичко значење и побаруваат навремена координација и одговор[xliii].

Планот зема предвид збир на водечки начела (пропорционалност, супсидијарност, комплементарност и доверливост на информациите), ги претставува основните цели на соработката (ефективен одговор, споделена свесност за ситуацијата, пораки на јавноста) на три нивоа (стратешко/политичко, оперативно и техничко), механизмите и вклучените актери, како и активностите за исполнување на наведените основни цели[xliv].

8.2.1. Клучни мерки

- МДТ како Орган за координирање и управување со инциденти со голем опфат и кризи;
- План за координиран одговор на големи инциденти и кризи, кој ќе вклучи процедури за справување со кризи.

8.3. Посебна цел 3. Навремено и соодветно справување со сајбер криминал

Инцидентите поврзани со сајбер безбедноста често преминуваат во компјутерски криминал, а притоа имаат големо влијание врз јавниот и приватниот сектор. Во овој контекст, Министерството за внатрешни работи и Секторот за компјутерски криминал имаат клучна улога во управувањето и решавањето на овие предизвици. За успешно справување со овие закани, Стратегијата за сајбер безбедност 2025 - 2028 година предвидува засилена соработка со секторите со висока критичност и надлежните органи, со фокус на координација и брза реакција на сајбер криминал.

Формирањето Постојана работна група за соработка на МВР со Националниот CSIRT и Владиниот CSIRT при МДТ, ќе ги забрза размената на информации и заедничкиот координиран одговор на сајбер инциденти и компјутерски криминал. Покрај тоа, креирањето единствена точка за пријавување сајбер инциденти и компјутерски криминал ќе овозможи ефективна комуникација и одговор со другите засегнати страни.

Соработката со меѓународни организации од областа на компјутерски криминал и безбедност, какви што се Интерпол и Европол, ќе обезбеди важни информации и насоки за справување со компјутерскиот криминал. Воедно, ќе се спроведуваат кампањи за подигање на јавната свест, за сајбер безбедност поврзано со компјутерски криминал.

Изготвувањето на нова Стратегија за компјутерски криминал, со акцент на соработка и координација со различни институции и вклучување во меѓуинституционални партнерства, е

клучен чекор во справувањето со овие предизвици. Цел на оваа стратегија ќе биде не само откривање и спречување сериозни форми на компјутерски криминал, туку и придонес за заштита на критичната ИКТ-инфраструктура и системи во државата.

Стратегијата предвидува формирање меѓународни партнерства за следење и процесирање на онлајн криминал против деца.

8.3.1. Клучни мерки

- Унапредување на капацитетите за справување со сајбер криминал;
- Хармонизација на националните со меѓународните политики поврзани со сајбер криминал;
- Воспоставување ефикасни процедури за пријавување и истражување сајбер криминал;
- Обезбедување стручно-специјалистичко образование и обука за лицата што работат во областа на идентификација и истражување сајбер криминал;
- Спроведување кампањи за сајбер безбедност поврзани со компјутерски криминал;
- Континуирана процена на соодветноста и ефективноста на националната регулатива за сајбер криминал;
- Континуирана едукација на правосудните органи во областа на сајбер безбедност, сајбер криминал и електронски докази.
- Нова Стратегија за сајбер криминал;
- Спроведување кампањи за сајбер безбедност поврзани со компјутерски криминал;
- Меѓународни партнерства за следење и процесирање на онлајн криминали против деца.

9. Приоритетна област 5: Национална и меѓународна соработка

Општа цел: Јакнење на националните капацитети и градење доверба во сајбер просторот.

Државата преку партнерства со приватниот сектор и со меѓународните сојузници ќе ја зајакне својата отпорност на сајбер напади и инциденти. Меѓуинституционалната соработка и соработката помеѓу јавниот и приватниот сектор е еден од основните предуслови за градење општество што успешно ќе се справува со предизвиците што ги носи дигитализацијата.

Меѓународната соработка е еден од клучните сегменти во заложбите за зголемување на капацитетите за справување со заканите во сајбер просторот, особено во делот на размена на информации, искуства и добри практики.

Во меѓународниот дијалог, Република Северна Македонија се залага за доследно спроведување отворена размена на информации и слобода на изразување и ја нагласува недискриминацијата. Договорите и стандардите што се однесуваат на меѓународното право се применливи и за сајбер доменот.

Надворешнополитичките инструменти какви што се дипломатската комуникација, предупредувањата и санкциите може значајно да придонесат за ограничување и ублажување на штетите предизвикани од сајбер нападите и за нивна превенција и спречување.

9.1. Посебна цел 1. Соработка на полето на сајбер безбедноста на национално, регионално и меѓународно ниво

Националниот совет за дигитална трансформација на општеството преку својата работна група за сајбер безбедност, како и други работни групи за сајбер и информациска безбедност, за

безбедност на критична информациска инфраструктура (CICWG) под раководство на МДТ, се клучни за координација на соработката помеѓу јавниот и приватниот сектор. Единствената точка за контакт ќе биде задолжена за комуникација и размена на информации во државата, како и за меѓународната соработка во областа на сајбер безбедност.

Република Северна Македонија ќе продолжи да гради билатерални и мултилатерални партнерства и да биде дел од заеднички платформи на регионално и на меѓународно ниво, за справување со сајбер заканите.

9.1.1. Клучни мерки

- Соработка во рамките на НАТО и ЕУ, земјите од регионот, други земји и релевантните меѓународни организации;

9.2. Посебна цел 2. Одговорно однесување на државата и мерки за градење доверба во сајбер просторот

Преку резолуција, Генералното собрание на Обединетите нации формираше отворена работна група (OEWG), во која сите земји членки на ОН, каде што член е и Република Северна Македонија, на 31 декември 2020 година, ја донесе резолуцијата 75/240 1 за формирање отворена работна група за безбедност и користење на информатичките и на комуникациските технологии со мандат од 5 години (2021-2025). Република Северна Македонија во иста линија со ЕУ и земјите членки се усогласи со коментарите и предлозите споделени од земјите членки и ја даде својата согласност за усвојување на финалната верзија на Резолуцијата на Генералното собрание над годишниот извештај за напредок.

Република Северна Македонија ќе се стреми во исполнување на главните точки што беа усвоени во ова собрание. Во овој контекст, Република Северна Македонија, исто така, останува посветена на имплементацијата на 16-те Мерки за градење доверба од ОБСЕ, чија цел е намалување на ризикот од конфликт што би произлегол од употребата на информациско-комуникациски технологии.

9.2.1. Клучни мерки

- Промовирање на нормите, на правилата и на начелата на одговорно однесување од страна на државата, во согласност со утврдените начела на меѓународно ниво.
- Заштита на националните интереси преку учество во дефинирањето на меѓународните правни акти поврзани со начинот на однесување во сајбер просторот, слободата на изразување, заштитата на личните податоци, правата на приватност и основните човекови права и слободи;

10. Рамка за следење, оценување и известување

10.1. Показатели на успешност за следење на постигнување на целите

Рамката за следење на постигнување на целите на Стратегијата за сајбер безбедност 2025 - 2028 годинасе заснова на показателите на успешност (KPI) и показатели за постигнување на целта (KGI) дефинирани на ниво на цели, мерки и задачи утврдени во Стратегијата за сајбер безбедност 2025 - 2028 годинаи Акцискиот план.

10.2. Имплементација на Стратегијата за сајбер безбедност

Стратегијата за сајбер безбедност 2025 - 2028 годинаќе се имплементира во текот на четири години, од 2025 до 2028 година, според целите, мерките и активностите што се детално наведени во Акцискиот план.

Следењето и известувањето за процесот на имплементација на Стратегијата за сајбер безбедност 2025 - 2028 година ги спроведува МДТ, кое ќе биде одговорно за севкупното спроведување на Стратегијата за сајбер безбедност 2025 - 2028 година.

Следењето на процесот на имплементација на Стратегијата за сајбер безбедност 2025 - 2028 година ќе се врши преку собирање податоци за степенот на реализација на активностите и преку утврдување на евентуалните ризици што можат да произлезат од нереализирани активности или од неостварените резултати, од сите засегнати страни што учествуваат во активностите предвидени во Стратегијата за сајбер безбедност 2025 - 2028 година.

МДТ до Владата на Република Северна Македонија ќе доставува полугодишни и годишни извештаи со податоци за степенот на реализација на Акцискиот план на Стратегијата за сајбер безбедност 2025 - 2028 година. Извештаите ќе се објавуваат на веб-страницата на МДТ.

МДТ преку работна група составена од претставници на засегнати страни во државата, ќе спроведува годишна ревизија на Стратегијата за сајбер безбедност 2025 - 2028 година и Акцискиот план. Ревизијата ќе има за цел утврдување на степен на реализација на планираните активности и ажурирање на текстот на Стратегијата за сајбер безбедност 2025 - 2028 година , Акцискиот план и пропратните документи, согласно Методологијата за начинот на известување и оценување на секторските стратегии, и Упатството за структурата, содржината и начинот на подготвување, спроведување, следење, известување и оценување на секторските и мултисекторските стратегии. Исто така ажурирањето на Акцискиот план ќе се врши согласно член 43 од Упатството за структурата, содржината и начинот на подготвување, спроведување, следење, известување и оценување на секторските и мултисекторските стратегии. Процесот ќе се одвива во согласност со обврските наведени врз основа на актуелните случувања во сајбер-просторот и предлозите од членовите на работната група.

На овој начин ќе се обезбеди преглед за степенот на реализација по целите на Стратегијата за сајбер безбедност 2025 - 2028 година и ќе се потврдат плановите и активностите за нејзина понатамошна реализација.

10.3. Засегнати страни

МДТ, како носител на имплементацијата на Стратегијата за сајбер безбедност 2025 - 2028 година, ќе соработува со Владата на Република Северна Македонија, со Советот за дигитална трансформација на општеството и со сите засегнати страни вклучени во имплементацијата на Стратегијата за сајбер безбедност 2025 - 2028 година, со цел квалитетна и навремена реализација на активностите предвидени во Акцискиот план на Стратегијата за сајбер безбедност 2025 - 2028 година.

Бидејќи сајбер безбедноста е одговорност на сите, освен ангажманот на МДТ, на Владата на Република Северна Македонија и на државните институции, од големо значење ќе биде придонесот од приватниот сектор, донаторите, академскиот сектор, истражувачките организации, невладиниот сектор и други организации, како засегнати страни во остварување на целите на Стратегијата за сајбер безбедност 2025 - 2028 година. Следува список на органи и

засегнати страни вклучени во спроведувањето на Стратегијата за сајбер безбедност 2025 - 2028 година:

- Национален совет за безбедност
- Влада на Република Северна Македонија
- Национален совет за дигитална трансформација на општеството
- Национален совет за ИКТ
- Министерство за дигитална трансформација
- Министерство за внатрешни работи
- Министерство за одбрана
- Министерство за правда
- Министерство за надворешни работи и надворешна трговија
- Министерство за образование и наука
- Министерство за енергетика, минерални суровини и рударство
- Министерство за финансии
- Министерство за транспорт
- Министерство за јавна администрација
- Министерство за труд и социјална политика
- Армија на РСМ
- Биро за развој на образованието
- Универзитети - Универзитет „Св. Кирил и Методиј“ – Скопје, Универзитет „Св. Климент Охридски“ – Битола, Универзитет „Гоце Делчев“ – Штип, Државен универзитет во Тетово, Универзитет за информатички науки и технологии „Св. Апостол Павле“ – Охрид, Универзитет „Мајка Тереза“ – Скопје, Универзитет на Југоисточна Европа - Тетово.
- Агенција за електронски комуникации, Национален центар за одговор на компјутерски инциденти, МКД - ЦИРТ
- Центар за управување со кризи
- Агенција за заштита на лични податоци
- Агенција за национална безбедност
- Дирекција за безбедност на класифицирани информации
- Агенција за разузнавање
- Академија за судии и јавни обвинители
- Министерство за локална самоуправа

11. Управување со ризици

Во ова поглавје се идентификувани главните ризици, на највисоко ниво. Препорака е, при имплементација на секоја посебна активност од Стратегијата за сајбер безбедност 2025 - 2028 година, носителот на активноста да води посебен регистар за ризици, со што ќе се предвидат чекори за избегнување на секој поединечен ризик, а во зависност од веројатноста да се случи и ефектот што ќе го има на имплементацијата на соодветната активност, да се планираат и акции и финансиски средства за минимизирање на ефектот од тој ризик.

Ризик 1. Отсуство на поддршка за реализација на Стратегијата за сајбер безбедност 2025 - 2028 година

Отсуството на политичка поддршка од сите засегнати страни и релевантни чинители во процесот за целосно воспоставување структури за управување со сајбер безбедност во државата кои се

предвидени со Стратегијата за сајбер безбедност 2025 - 2028 годинае клучен ризик за неисполнување на заложбите од Стратегијата за сајбер безбедност 2025 - 2028 година.

За надминување на овој ризик, потребна е целосна политичка поддршка и добра координираност на сите чинители во процесот на креирање и поставување на структурите за управување со сајбер безбедност како основа за исполнување на стратешките цели, а пред сè за воспоставување здрав и безбеден сајбер простор, кој ќе биде отпорен на сајбер ризици подготвен ефективно и ефикасно да одговори на евентуалните сајбер напади.

Ризик 2. Недостиг на финансиски средства

Имајќи ја предвид моменталната ситуација во државата и буџетите со кои располагаат државните институции, постои реален ризик од недостиг на буџетски средства за имплементација на Стратегијата за сајбер безбедност 2025 - 2028 година.

За надминување на овој ризик, ќе се прави редовно приоритизирање на активностите и по потреба прераспределба на планираните буџетски средства за имплементација на оние мерки и задачи што се со највисок приоритет. Дополнително, за задачите каде што е тоа применливо, ќе се бара дополнителна донаторска помош за нивна реализација.

Ризик 3. Недостиг на човечки капацитети и експерти за сајбер безбедност

Недостигот на квалификуван и професионален ИКТ-кадар, особено на професионалци со познавање сајбер безбедност, е сè поизразен, не само во државата туку и во регионот и пошироко, така што претставува голем ризик за неисполнување одредени цели од Стратегијата за сајбер безбедност 2025 - 2028 година.

За надминување на овој ризик, Владата на Република Северна Македонија ќе работи на изнаоѓање модалитети за мотивирање и задржување на професионалците за сајбер безбедност, а истовремено да се овозможи зголемено ниво на иновациски активности кај бизнисите. Дополнително, а и како важна цел во Стратегијата за сајбер безбедност 2025 - 2028 година, Владата на Република Северна Македонија и државата стават фокус на обука, специјализација и преквалификација на постојните човечки ресурси во насока на нивно стручно оспособување за работа во областа на сајбер безбедност.

Ризик 4. Глобални кризи и природни катастрофи

Глобалните економски, безбедносни и здравствени кризи, како и природни катастрофи (земјотреси, поплави, пожари), претставуваат ризик што, доколку се случи, може да има големо влијание и негативен ефект на реализацијата на целите на Стратегијата за сајбер безбедност 2025 - 2028 година.

Поради тоа што глобалните кризи и природни катастрофи тешко може да се предвидат, а уште помалку да се контролираат, важно е Владата на Република Северна Македонија да настапи со превентивни мерки, кои ќе придонесат за полесно справување со ситуацијата, доколку дојде до кризи и инциденти со голем опфат. Тоа значи добро дефинирани процедури за работа и постапување во случај на кризи и инциденти со огромен опфат, обезбедување континуитет во работењето и обука на кадрите за работа во случај на кризи и инциденти со голем опфат.

Образец бр. 4, УТВРДУВАЊЕ НА РИЗИЦИ

РИЗИК	ВЕРОЈАТНОСТ ЗА НАСТАНУВАЊЕ НА РИЗИКОТ	ВЛИЈАНИЕ НА РИЗИКОТ ВРЗ ОСТВАРУВАЊЕ НА ЦЕЛИТЕ	МЕРКИ ЗА СПРАВУВАЊЕ СО РИЗИКОТ
Отсуство на поддршка за реализација на Стратегијата за сајбер безбедност 2025 - 2028 година	Средна	Големо	- Обезбедување целосна политичка поддршка од сите релевантни чинители. - Добра координираност на институциите. - Јакнење на структурите за управување со сајбер безбедност.
Недостиг на финансиски средства	Голема	Големо	- Приоритизација на активности и прераспределба на буџетските средства. - Обезбедување дополнителна донаторска поддршка. - Оптимизација на расходите за критичните задачи.
Недостиг на човечки капацитети и експерти за сајбер безбедност	Голема	Големо	- Мотивирање и задржување на професионалците за сајбер безбедност. - Обука, специјализација и преквалификација на кадри. - Поттикнување на иновации во бизнис секторот.
Глобални кризи и природни катастрофи	Средна	Големо	- Развивање на процедури за справување со кризи.

			- Обезбедување на континуитет во работењето. - Обука на кадрите за работа во услови на кризни ситуации.

12. Акциски План

Акцискиот план е даден во Прилог - Образец бр. 3 Акциски план за спроведување на Стратегијата за сајбер безбедност 2025 - 2028 година.

13. Индикативен финансиски план

Финансиските ресурси за имплементација на сите активности вклучени во Акцискиот план на Стратегијата за сајбер безбедност 2025 - 2028 годинаќе бидат планирани соодветно со индикативните буџети и ќе бидат обезбедени од буџетот на носителот на активноста наведени во Акцискиот план.

Потенцијални идни кризни мерки и ризици од скратување на годишниот буџет, за одредени активности содржани во Акцискиот план, а чија природа го дозволува тоа, не е исклучено да се јави потреба од донаторска поддршка за дополнување на државните средства.

Заклучок

Пред вас е стратешки документ, Стратегијата за сајбер безбедност 2025 - 2028 година, изработен со голема посветеност на работната група, формирана од стручни лица од сите засегнати страни, раководена од МДТ.

Успешната имплементација на Стратегијата за сајбер безбедност 2025 - 2028 годинаи на Акцискиот план, ќе има позитивно влијание на зголемена сајбер безбедност и на тој начин дополнително ќе придонесе и на зголемување на целокупната безбедност во државата.

Со усвојувањето на Стратегијата за сајбер безбедност 2025 - 2028 година,Владата на Република Северна Македонија и засегнатите страни се обврзуваат да обезбедат финансиски средства и потребни ресурси за исполнување на целите, на мерките и на задачите од Стратегијата за сајбер безбедност 2025 - 2028 година, со што ќе придонесат за подобрување на отпорноста во сајбер просторот во Република Северна Македонија, со крајна цел Република Северна Македонија да биде безбедна и доверлива дигитална средина за онлајн дејствување и работа.

Анекс 1 – Список на сектори со висока критичност

До моментот на усвојување на овој документ, Република Северна Македонија нема важечки закон со кој се идентификувани критичните сектори во државата. Од оваа причина Списокот на други критични сектори е во согласност со Анекс 2 од европската Директива (EU) 2022/2555.

Сектор	Потсектор
Енергија	(а) Електрична енергија
	(б) Централно греење и ладење
	(в) Нафта
	(г) Гас
	(д) Водород
Транспорт	(а) Воздух
	(б) Железница
	(в) Вода
	(г) Пат
Банкарство	
Инфраструктури на финансискиот пазар	
Здравје	
Вода за пиење	
Отпадна вода	
Дигитална инфраструктура	
Управување со ИКТ-услуги	
Јавен сектор (јавна администрација)	Институции од централна власт
	Институции од локална власт
Вселена	

Анекс 2 – Список на други критични сектори

Република Северна Македонија нема важечки закон со кој се идентификувани критичните сектори во државата. Од оваа причина Списокот на други критични сектори е во согласност со Анекс 2 од европската Директива (EU) 2022/2555.

Сектор	Потсектор
Поштенски и курирски услуги	
Управување со отпад	
Изработка, производство и дистрибуција на хемикалии	
Производство, обработка и дистрибуција на храна	
Производство	(а) Производство на медицински помагала и медицински помагала за дијагностика ин витро
	(б) Производство на компјутерски, електронски и оптички производи
	(в) Производство на електрична опрема
	(г) Производство на машини и опрема
	(д) Производство на моторни возила, приколки и полуприколки
	(ѓ) Производство на друга транспортна опрема
Даватели на дигитални услуги	
Истражување	

Анекс 3 – Дефиниции

Академија претставува образовна или истражувачка институција, универзитет или друга стручна установа која игра клучна улога во едукацијата, обуката и развојот на човечки ресурси во областа на сајбер безбедноста. Академијата служи како партнер во создавање на експертски кадар, спроведување научни истражувања и промовирање на свесност и знаење за сајбер безбедност во општеството.

Аутсорсинг е практика на префрлување одредени функции или услуги на надворешни организации, со цел да се зголеми ефикасноста, да се намалат трошоците и да се подобри квалитетот на услугите, овозможувајќи на организацијата да се фокусира на своите основни активности.

Граѓански сектор се однесува на дел од општеството кој е составен од организации и иницијативи кои не се дел од државните институции или приватниот сектор. Овој сектор вклучува невладини организации (НВО), здруженија на граѓани, фондации, активистички групи и други колективи кои работат за решавање на општествени проблеми, промовирање на човековите права, заштита на животната средина, културни активности, и слични цели.

Дигитализација е процес на конвертирање физички информации, документи или процеси во дигитален формат. Оваа трансформација овозможува податоците да бидат лесно достапни, преносливи и обработливи со помош на компјутерски системи.

Дигитална инфраструктура се однесува на основните технолошки компоненти и ресурси потребни за функционирање и поддршка на дигиталните системи и услуги. Ова вклучува мрежна инфраструктура (какви што се интернет и локални мрежи), сервери, облачни услуги, софтверски апликации, бази на податоци и хардверски уреди.

Дигитална средина се однесува на виртуелниот простор создаден од компјутерски системи, интернет и дигитални технологии, каде што се комуницира, се разменува информации и се извршуваат различни активности. Оваа средина вклучува веб-страници, социјални мрежи, онлајн платформи, апликации и дигитални уреди.

Дигитална трансформација е процес на интеграција на дигитални технологии во сите области на работењето, преку дигитален бизнис-модел.

Дигитални права се права и слободи што се однесуваат на користењето на дигиталните технологии и интернетот, вклучувајќи право на приватност, слобода на изразување, пристап до информации и безбедност, со цел да се заштитат индивидуалните интереси и слободи во дигиталната средина.

Злонамерен софтвер (malware) – софтвер што е специјално дизајниран да го наруши, оштети, или да добие овластен пристап до информациски систем.

Индустриски контролни системи – информациски системи во SCADA (надзорна контрола и собирање податоци) и групите за дистрибуирани контролни системи, кои се користат за индустриски операции, какви што се производство, контролирање на производството и контрола на дистрибуцијата преку програмски логички контролери, кои се различни од конвенционалните информатички технологии.

Инцидент е настан што се случува, често непријатен или неочекуван, кој може да доведе до проблеми или нарушување на нормалниот тек на работите.
Интернет е глобална компјутерска мрежа што обезбедува поврзување на информациски и комуникациски уреди и системи поврзани со користење стандардизирани комуникациски протоколи.

Интернет-провајдери се компании или организации што нудат услуги за пристап до интернет, овозможувајќи им на корисниците да се поврзат на глобалната мрежа. Тие може да понудат различни видови услуги, вклучувајќи широкопојасен интернет, мобилен интернет, виртуелни приватни мрежи (VPN) и хостинг услуги.

Информациска безбедност Заштита на информациите и информациските системи од неовластен пристап, употреба, откривање, нарушување, модификација или уништување со цел да се обезбеди доверливост, интегритет и достапност.

Информациско-комуникациски технологии (ИКТ) се технологии што овозможуваат собирање, обработка, чување и пренос на информации, вклучувајќи компјутери, интернет, софтвер и комуникациски алатки, и играат клучна улога во модерното општество за поддршка на комуникацијата и управувањето со податоци.

Класифицирана информација –е информација од делокругот на работа на орган на државната и локалната власт основан согласно со Уставот на Република Северна Македонија и со закон, правно лице основано од Републиката или од општините, градот Скопје и општините во градот Скопје или други правни лица којашто се однесува на јавната безбедност, одбраната, надворешните работи или безбедносни или разузнавачки активности на државата која согласно со закон мора да се заштити од неовластен пристап и е обележана со соодветен степен на класификација согласно Законот за класифицирани информации(*) („Службен весник на РСМ“, бр. 275/19)

Критична информациска инфраструктура (КИИ) – кои било информациско-комуникациски системи чиешто одржување, сигурност и безбедност се критични за националната безбедност, економијата, јавната безбедност и здравје. Националната критична информациска инфраструктура е дел од критична инфраструктура (КИ).

Личен податок –е секоја информација која се однесува на идентификувано физичко лице или физичко лице што може да се идентификува (субјект на лични податоци), додека физичко лице што може да се идентификува е лице чијшто идентитет може да се утврди, директно или индиректно.

Национална безбедност – систем за современ облик на организирање и функционирање на општеството заради спроведување специфични активности и мерки на превентивен и репресивен план во функција на заштита на фундаменталните општествени вредности од сите видови и облици на безбедносни предизвици, закани и ризици на сите нивоа.

Националните мрежи и информациски системи се структури и платформи што овозможуваат размена на информации и комуникација помеѓу различни владини институции и агенции, како и помеѓу државните органи и граѓаните. Овие мрежи и системи вклучуваат инфраструктура за компјутерски мрежи, софтверски решенија за управување со податоци и системи за обезбедување на информациите. Нивната главна цел е да се подобри ефикасноста на јавната администрација, да се зголеми транспарентноста и одговорноста, и да се олесни пристапот до јавните услуги за граѓаните.

Надлежни органи – органи на државна управа, други државни органи, органи во состав на министерствата, управни организации и самостојни органи, правосудни органи и судови, органи на општините, на Градот Скопје и на општините на градот Скопје, како и правни и други лица на кои со закон им е доверено да вршат јавни овластувања. Во овој контекст терминот други субјекти се однесува на: правни лица што даваат и обезбедуваат услуги од јавен интерес, односно субјекти од областа на образованието, здравството, финансиите, банкарството, осигурувањето, енергетиката, водоснабдувањето, електронските комуникации, поштенските услуги и комуналните услуги.

Надлежни органи (во контекст на Стратегијата за сајбер безбедност 2025 - 2028 година и во согласност со НИС2) – надлежни органи во согласност со Директивата за мрежи и информациски системи 2 (НИС2) се институции назначени од државите членки на Европската Унија за спроведување на мерките за безбедност на мрежите и на информациските системи. Тие имаат задача да обезбедат усогласеност со законодавството, да надгледуваат и да оценуваат безбедносните ризици, да спроведуваат инспекции и да координираат одговори на инциденти во сајбер безбедноста, со цел да се заштити инфраструктурата и податоците од закани и напади.

Органи на државната управа се институции основани со закон за извршување на функции од извршната власт, управни и стручни работи. Тие можат да бидат министерства или други органи поделени на самостојни (дирекции, архиви, агенции, комисии) и органи во состав на министерствата (управи, бироа, служби, инспекторати, капетании)

Приватен сектор е дел од економијата составен од организации и компании што се во сопственост на индивидуални или правни лица, а не на државата. Овој сектор се сосредоточува на генерирање профит преку производствени и услужни активности, и вклучува мали, средни и големи бизниси.

Робустен/робусност означува својство на систем, организација или процес да биде отпорен на нарушувања, да функционира стабилно во услови на промени и да закрепне од непредвидливи ситуации. Робусни системи се способни да одржат својата ефикасност и функционалност, дури и кога се соочуваат со предизвици или ризици.

Свесност – се однесува на безбедносната свесност на сите лица што споделуваат одговорност за безбедноста на информациите.

Сајбер безбедност е практика на заштита на мрежи, уреди и податоци од неовластен пристап или криминална употреба и обезбедување доверливост, интегритет и достапност на информациите. Покрај терминот сајбер безбедност некаде се користи и терминот кибер безбедност.

Сајбер булинг е облик на малтретирање, кој се одвива преку дигитални платформи, какви што се социјални мрежи, текстуални пораки, е-пошта и други онлајн канали. Овој вид малтретирање може да вклучува праќање заканувачки или навредливи пораки, ширење лажни информации, објавување срамни фотографии или создавање лажни профили.

Сајбер екосистем е комплексен систем што вклучува различни елементи, какви што се технологија, инфраструктура, корисници, органи за регулирање и услуги, кои сите заедно функционираат во дигиталната средина. Целта на сајбер екосистемот е да обезбеди безбедна, ефикасна и инклузивна дигитална средина, каде што поединци и организации можат да комуницираат и да разменуваат информации безбедно и доверливо.

Сајбер закана – потенцијалната причина за инцидент во сајбер просторот што може да предизвика оштетување на некоја институција или систем.

Сајбер инцидент – е настан што ја загрозува достапноста, интегритетот или доверливоста на информациите или информатичките (ИКТ) системи.

Сајбер инцидент од голем опфат – сајбер инцидент што предизвикува ниво на нарушување што го надминува капацитетот на земјата да одговори на него или што има значително влијание и во најмалку уште една друга земја.

Сајбер криза – настан или настани во сајбер просторот кои би можеле да предизвикаат или веќе предизвикале значително нарушување во општествениот, политичкиот и во економскиот живот на Република Северна Македонија. Ваквата ситуација може да влијае врз безбедноста на граѓаните, демократскиот систем, политичката стабилност, економијата, животната средина и другите национални вредности, односно националната безбедност и одбраната воопшто.

Сајбер криминал – различни криминални активности каде што информациските системи се вклучени или како примарна алатка или како примарна цел на напад.
Сајбер напад – операции што лицата и/или информатичките системи намерно ги вршат на кое било место во сајбер просторот со цел да се загрозат доверливоста, интегритетот или достапноста на информативните системи во националниот сајбер простор.

Сајбер одбрана – проактивна мерка за откривање или добивање информации во врска со сајбер упад, сајбер напад или сајбер операција или за утврдување на потеклото на операцијата што вклучува инволвирање превентивна или сајбер контра операција против изворот.

Сајбер отпорност – способноста да се подготви, да се приспособи, да издржи и брзо да закрепне од нарушувања што произлегуваат од намерни напади, несреќи или природни закани или инциденти во сајбер просторот.

Сајбер професионалци се стручни лица што се занимаваат со безбедноста на компјутерските системи, мрежи и податоци. Нивната работа вклучува заштита од сајбер напади, идентификување безбедносни закани, развој на безбедносни политики и процедури, како и одговор на инциденти.

Сајбер ризик – потенцијален ризик од предизвикување штета со користење слабости во еден или повеќе информациски субјекти.

Сајбер шпионажа е сајбер напад насочен против доверливоста на ИКТ-системите.

Стопански комори се независни, непрофитни и доброволни организации кои ги обединуваат деловните субјекти со цел застапување на нивните интереси, унапредување на стопанството и поддршка на економскиот развој. Тие обезбедуваат платформа за соработка, услуги за членовите и промовирање на дијалог меѓу приватниот и јавниот сектор. Во Република Северна Македонија постојат неколку значајни комори, како што се Стопанската комора на Северна Македонија, Комората на северозападна Македонија, Сојузот на стопански комори на Македонија, МАСИТ – Стопанска комора за ИКТ и МАКАМ-ТРАНС – Стопанска комора за транспорт, кои играат клучна улога во поддршката на деловната заедница и економијата.

Хибридно војување е стратегија што комбинира традиционални воени операции со нетрадиционални тактики и алатки, какви што се сајбер напади, дезинформации, економски притисоци и поддршка на неформални вооружени групи.

Хибридни закани се ситуации или активности што комбинираат традиционални и нетрадиционални методи за предизвикување нестабилност или опасности, какви што се воени инвазии, сајбер напади, дезинформации, економски санкции и поддршка на парамилитарни групи. Овие закани се сложени и тешко предвидливи, што ги прави особено опасни за националната безбедност и стабилност.

CSIRT (Computer Security Incident Response Team) е специјализирана група или тим што управува и реагира на инциденти од сајбер безбедноста за да го намали нивното влијание и да ја подобри безбедноста во иднина.

SOC (Security Operation Center) – структура или функција на суштински или важен субјект, или организација, кој е задолжен за активности поврзани со сајбер и информациската безбедност на организацијата. Дејствува превентивно и реактивно. CSIRT може да биде составен дел на SOC.

Јавен сектор се органите на државната власт и други органи и организации утврдени со закон, органите на општините, градот Скопје и општините во градот Скопје, установите и јавните служби, јавните претпријатија, правни и физички лица што вршат јавни овластувања утврдени со закон.

Анекс 4 – Акроними

АРСМ – Армија на Република Северна Македонија

ИТ – Информациски технологии

ИКТ – Информациско-комуникациски технологии

КИИ – Критичната информациска инфраструктура

НСДТО – Национален совет за дигитална трансформација на општеството

НРУСБ - Национална рамка за управување со сајбер безбедност

МДТ – Министерство за дигитална трансформација

МНРНТ – Министерство за надворешни работи и надворешна трговија

МСПДМ – Министерство за социјална политика, демографија и млади

МОН – Министерство за образование и наука

МВР – Министерство за внатрешни работи

ЦРСО - Центар за развој на стручното образование,

ОТ – Оперативни технологии

РСМ – Република Северна Македонија

ССБ – Сектор за сајбер безбедност при МДТ

CERT – (Computer Emergency Response Team) Тим за одговор на компјутерски вонредни ситуации

CIRT – (Computer Incident Response Team) Тим за одговор на компјутерски инциденти

CSIRT – (Computer Security Incident Response Team) Тим за одговор на компјутерски безбедносни инциденти

SCADA – (Supervisory Control and Data Acquisition) е систем што се користи за контрола на индустриските процеси од далечина преку собирање и анализа на податоци во реално време.

ЕУ – Европска Унија

НАТО – Организација на Северноатлантскиот договор

МКД-ЦИРТ – Национален центар за одговор на компјутерски инциденти

USAID – (United States Agency for International Development) Американска агенција за меѓународен развој

DCAF – (Geneva Centre for Security Sector Governance) Женевски центар за управување со безбедносниот сектор

SOC – (Security operations center) Центар за оперативна безбедност

ISO – (International organization for standardization) Меѓународна организација за стандардизација

NIST – (National institut for standards and technology) Национален институт за стандарди и технологија

ЈПП – јавни-приватни партнерства

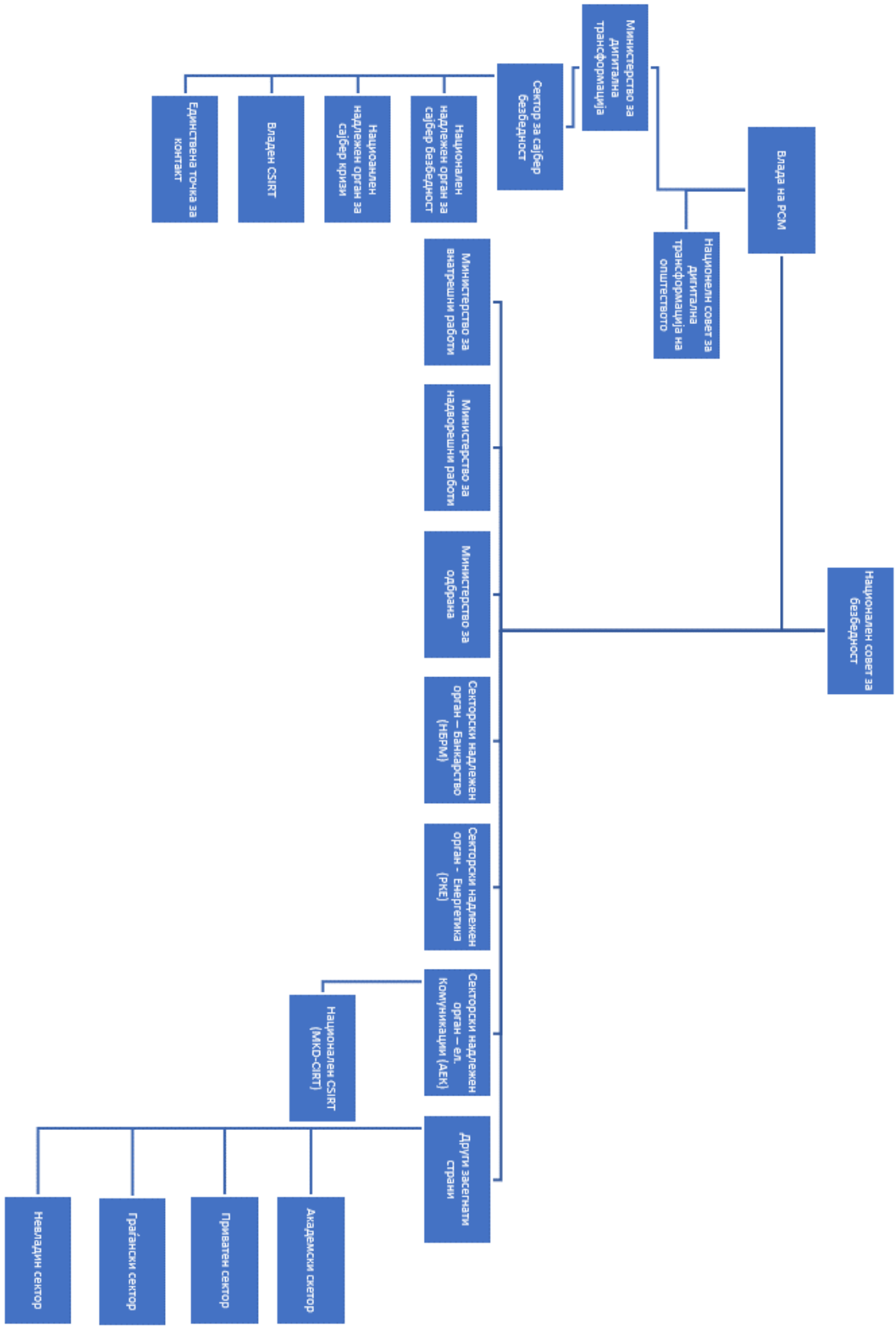
ITU – (Intenrational Telecommunications Union) Меѓународна телекомуникациска унија

ENISA – (European Cybersecurity Agency) Агенција за сајбер безбедност на Европската Унија

SPOC (Single Point of Contact) – Национална Единствена точка за контакт

НИС 2 (Network and Information Systems Directive 2) – Директива за мрежи и информациски системи 2

Анекс 5 – Предлог за Поставеност на субјекти и функции во Националната рамка за управување со сајбер безбедноста



Анекс 6 – Список на користени информации и референци

[i] ITU, https://www.itu.int/pub/D-STR-CYB_GUIDE.01, Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity.
[ii] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools
[iii] https://vlada.mk/sites/default/files/dokumenti/informacija_i_metodologija.pdf
[iv] https://vlada.mk/konceptDT
[v] 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), https://eur-lex.europa.eu/eli/dir/2022/2555/oj
[vi] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, https://eur-lex.europa.eu/eli/dir/2022/2557/oj
[vii] 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) (Text with EEA relevance), https://eur-lex.europa.eu/eli/reg/2019/881/oj
[viii] https://zelenaberza.com.mk/mvr-postapuva-po-hakerskiot-napad-vo-ministerstvoto-za-zemjodelstvo-koj-bara-otkup/
[ixix] https://telma.com.mk/2023/02/16/it-sistemot-na-fondot-za-zdravstvo-e-osvoen-od-hakeri-koi-baraat-otkup-potvrdi-i-kovachevski/
[x] https://www.slobodnaevropa.mk/a/32852038.html
[xi] https://dzr.mk/mk/240624-it-revizija-2023-efektivnost-na-prezemenite-merki-na-nadlezhnite-organi-za-zashtita-na
[xii] https://ener.gov.mk/default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=80751
[xiii] https://mvr.gov.mk/Upload/Editor_Upload/AP%20v1_13MK.pdf
[xiv] https://www.mchamber.mk/mk/home/propisi_info/962
[xv] https://mkd-cirt.mk/
[xvi] Стр. 8, Директива (EU) 2022/2555(https ://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555).
[xvii] Директива (EU) 2022/2555(https ://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555)
[xviii] Закон за трговските друштва – консолидиран текст, https://www.economy.gov.mk/Upload/Documents/ZTD%20konsolidiiran.pdf
[xix] Директива (EU) 2022/2555, стр. 30
[xx] Директива (EU) 2022/2555, стр. 30
[xxi] Директива (EU) 2022/2555, стр. 16
[xxii] Директива (EU) 2022/2555, стр. 16
[xxiii] Директива (EU) 2022/2555, стр. 16
[xxiv] Директива (EU) 2022/2555, стр. 16
[xxv] Директива (EU) 2022/2555, стр. 16
[xxvi] Директива (EU) 2022/2555, стр. 8.
[xxvii] Директива (EU) 2022/2555, стр. 39.
[xxviii] (ДИРЕКТИВА (EU) 2022/2555 Директива, член 10, Стр. 38).
[xxix] Стр. 55, Директива (EU) 2022/2555(https://eur-lex.europa.eu/legal-content /EN/TXT/?uri=CELEX%3A32022L2555).
[xxx] (ДИРЕКТИВА (EU) 2022/2555, стр. 28, член 1)
[xxxi] (ДИРЕКТИВА (EU) 2022/2555, Стр 36, член 8)
[xxxii] (ДИРЕКТИВА (EU) 2022/2555, Стр 36, член 8)
[xxxiii] (Директива (EU) 2022/2555, стр. 36, член 8).
[xxxiv] Директива (ЕУ) 2022/2555, член 1.
[xxxv] Директива (ЕУ) 2022/2555, член 1.
[xxxvi] Директива (ЕУ) 2022/2555, член 1.
[xxxvii] Директива (ЕУ) 2022/2555, член 1.
[xxxviii] Директива (ЕУ) 2022/2555, член 3.
[xxxix] Директива (EU) 2022/2555, член 21.
[xl] Препорака на Комисијата (ЕУ) 2017 г. /1584, стр. 4.

[xli] Препорака на Комисијата (ЕУ) 2017/1584, стр. 1.
[xlii] Препорака на Комисијата (ЕУ) 2017/1584, стр. 1.
[xliii] Препорака на Комисијата (ЕУ) 2017/1584, стр. 5.
[xliv] Препорака на Комисијата (ЕУ) 2017/1584, стр. 5.