Република Македонија

Национална Стратегија за сајбер безбедност 2018-2022

Акциски План 2018-2022

Декември 2018 година

Вовед

Целта на овој документ е да ги дефинира чекорите во имплементацијата на првата Национална стратегија за сајбер безбедност на Република Македонија 2018-2022. По извршената анализа на капацитетите за сајбер безбедност на национално ниво, се оформи работна група одговорна за развивање на стратешки документи од областа на сајбер безбедноста, која вклучува претставници од трите надлежни министерства за сајбер безбедност во РМ - Министерството за информатичко општество и администрација, Министерството за одбрана и Министерството за внатрешни работи. Надлежноста на Работната група ќе се прошири и ќе го опфаќа спроведувањето на задачите кои се однесуваат на Телото со оперативни капацитети за сајбер безбедност, сè до основање на истото.

Овој Акциски план ги вклучува главните активности потребни за зајакнување на националните капацитети за сајбер безбедност. Меѓутоа, треба да се има предвид дека повеќето активности предвидени да бидат имплементирани од страна на Телото со оперативни капацитети за сајбер безбедност ќе бидат дополнително проверени и преоценети по воспоставувањето на ова тело.

Структурата на овој Акциски план вклучува три активности со највисок приоритет. Овие активности ја поставуваат основата на сите последователни активности, поделени според 5С цели дефинирани во Стратегијата. Активностите со висок, среден и низок приоритет се наведени под секоја од овие цели. За секоја активност се наведени задачи, предуслови, приоритет, одговорна институција, институции за соработка, извор на финансиски ресурси и временска рамка.

Имплементација

Национален совет за сајбер безбедност - трансформација на националниот Совет за ИКТ во Национален совет за ИКТ и безбедност

Националниот Совет за ИКТ е составен од министри, со што се обезбедува усогласеност при спроведување на стратешките одлуки на институционално ниво. Проширувањето на надлежностите на Советот за ИКТ ќе резултира со следните измени:

1. промена на името: Национален совет за ИКТ и безбедност
2. промена на надлежностите (информатичка бебедност како посебно поле во надлежност на Советот)
3. дополнителни членови во Советот, меѓу кои и идниот Директор на Телото со оперативни капацитети за сајбер безбедност

Телото со оперативни капацитети за сајбер безбедност* (кое ќе биде оформено во рамките на постоечки државен орган) ќе биде надлежно за имплементација на активностите во овој Акциски План, како и развој на оперативен план.

Напомена

*До формирање на ОТСБ, оваа активност ќе ја спроведува работната група задолжена за спроведување на активностите кои произлегуваат од стратешките документи за сајбер безбедност.

Акроними

АЕК - Агенција за електронски комуникации
АКВО - Агенција за квалитет на високо образование
АСЈО - Академија за судии и јавни обвинители
АРМ - Армија на Република Македонија
БРО - Биро за развој на образование
ВРМ - Влада на Република Македонија
ДЗЛП - Дирекција за заштита на личните податоци
ДБКИ - Дирекција за безбедност на класифицирани информации
Д.З. За Статистика - Државен завод за статистика
ДЗС - Дирекција за заштита и спасување
КИИ - Критичната информациска инфраструктура
КЗПВРМ за Економски прашања - Кабинет на Заменик претседател на Влада задолжен за економски прашања
ВИС – Важни информациски системи
ЕУ – Европска Унија
ЈО - Јавно обвинителство
МАСИТ - Стопанска комора за информатички и комуникациски технологии
МВР - Министерство за внатрешни работи

МЕ - Министерство за економија
МИОА - Министерство за информатичко општество и администрација
МКД-ЦИРТ - Национален центар за одговор на компјутерски инциденти
МНР - Министерство за надворешни работи
МО - Министерство за одбрана
МП - Министерство за правда
МФ - Министерство за финансии
МОН - Министерство за образование и наука
ИСБДФ - Национален институт за сајбер безбедност и дигитална форензика
НАТО – Организација на Северноатланскиот договор
НБРМ - Народна Банка на Република Македонија
НССБ - Национален Совет за сајбер безбедност
ОТСБ - Тело со оперативни капацитети за сајбер безбедност
СВБиР - Служба за воена безбедност и разузнавање
СЕП - Секретаријат за европски прашања
СЗ - Секретаријат за законодавство
ФИТР - Фонд за иновации и технолошки развој
ЦУК - Центар за Управување со кризи

CERT – Тим за одговор на компјутерски вонредни ситуации
CIRT – Тим за одговор на компјутерски инциденти
CSIRT – Тим за одговор на инциденти врз компјутерската безбедностWB6 -
WB6 - Western Balkans 6

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
ПРИОРИТЕТНИ АКТИВНОСТИ										
П1	Формирање на Национален Совет за сајбер безбедност	П1.1	Утврдување на надлежности на Националниот Совет за сајбер безбедност согласно Националната стратегија за сајбер безбедност		највисок	МИОА	Работна група за сајбер безбедност	/	Ноември 2018	Декември 2018
		П1.2	Идентификување на претседател и членови на Националниот Совет за сајбер безбедност							
		П1.3	Донесување на Решение за формирање Национален Совет за сајбер безбедност (или проширување на надлежности на постоечки совет)							
П2	Формирање на тело со оперативни капацитети за сајбер безбедност како новоформиран самостоен орган (агенција, дирекција) или како новоформирана организациска единица, односно орган во рамки на постоечки орган.	П2.1	Анализа на институционалните капацитети на постоечките органи и за утврдување на капацитетите со кои располага државата за формирање на тело со оперативни капацитети за сајбер безбедност.	П1	највисок	НССБ	МФ, надлежни министерства	Буџет на РМ	Јануари 2019	Јуни 2019
		П2.2	Утврдување на надлежности на телото со оперативни капацитети за сајбер безбедност согласно Националната стратегија за сајбер безбедност, притоа разграничувајќи ги со надлежностите на MKD-CIRT.							
		П2.3	Идентификување на потребните буџетски средства, просторни капацитети и човечки ресурси за формирање на телото со оперативни капацитети за сајбер безбедност, како и начинот на нивно обезбедување.							
		П2.4	Анализа на потребните законски измени и предлог текст за измени						Јули 2019	јануари 2020
		П2.5	Обезбедување на буџетски средства за формирање на тело							
		П2.6	Доставување на предлог за формирање на тело со оперативни капацитети за сајбер безбедност до Влада на РМ							
		П2.7	Донесување законска рамка за тело со оперативни капацитети за сајбер безбедност							
П3	Изработка на студија за идентификација на КИИ и ВИС	П3.1	Изработка на Студија за идентификација на КИИ и ВИС и потреба од транспонирање на ЕУ регулатива во оваа област. Резултатите од студијата треба да вклучат: 1. идентификувани сектори за КИИ 2. идентификувани надлежни авторитети/регулатори за секој сектор 3. идентификувани оператори на КИИ за секој сектор 4. проценка за потреба од измена на законска регулатива (lex generalis) за секој од идентификуваните сектори	П1	највисок	МИОА, MKD-CIRT	надлежни министерства, носители на КИИ и ВИС, Универзитети	Буџет на РМ, донаторска помош	Јануари 2019	април 2019

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
ЦЕЛ 1: САЈБЕР ОТПОРНОСТ										
1.1	Унапредување на капацитетите и способностите на MKD-CIRT и развој на останатите CSIRT/CERT/CIRT тимови.	1.1.1	Зголемување на број на вработени во центарот со доекипирање, пополнување на работни позиции и контунирана едукација на кадарот во делот на справување со инциденти, анализа на малвер, безбедносни проверки и форензика.	ПЗ	висок	MKD-CIRT	надлежни министерства, останати сектори, носители на КИИ и ВИС	Буџет на MKD-CIRT	2018г	2022г
		1.1.2	Проширување на бројот на понудени услуги согласно NIS директивата.	ПЗ	висок	MKD-CIRT, ОТСБ*	сите засегнати страни	Буџет на MKD-CIRT	2018г	2022г
		1.1.3	Развој на национална таксономија за сајбер инциденти.		висок	MKD-CIRT	Универзитети, МИОА	Буџет на MKD-CIRT	Јануари 2019	Јуни 2019
		1.1.4	Развој на дополнителни CSIRT/CERT/CIRT тимови на повеќе нивоа (секторски, институционални, академски итн.)		висок	сите организации и институции што имаат потреба и капацитет за развој на CSIRT/CERT/CIRT тимови	MKD-CIRT, ОТСБ*, надлежни министерства, носители на КИИ и ВИС, останати сектори	организациски и институционални буџети	2019	континуирано
1.2	Креирање единствена и сеопфатна правна рамка за сајбер отпорност, земајќи ја предвид позитивната законска регулатива во РМ и ЕУ.	1.2.1	Изработка и донесување на Закон за безбедност на мрежи и информациски системи со кој ќе се транспонира NIS директивата (ДИРЕКТИВА - ЕУ 2016/1148)		највисок	МИОА	сите засегнати страни	Буџет на РМ или донаторска помош	2019г	2020г
		1.2.2	Усогласување на домашното законодавство со NIS директивата.		висок	МИОА	надлежни министерства и сите останати засегнати страни	Буџет на РМ или донаторска помош	2020г	2021г
		1.2.3	Усогласување на Закон за управување со кризи земајќи ги во предвид ризиците за сајбер безбедноста.	ПЗ	висок	ЦУК, МО	MKD-CIRT, надлежни министерства	Буџет на РМ	2019г	2020г
1.3	Идентификација и заштита на КИИ (Критична информациска инфраструктура) и ВИС (други Важни Информациски Системи).	1.3.1	Дефинирање на листа на КИИ и ВИС врз основа на Студија за дефинирање и идентификација на КИИ и ВИС.	ПЗ	висок	МИОА	MKD-CIRT, универзитети, сите останати засегнати страни, носители на КИИ и ВИС	Буџет на РМ или донаторска помош	2019г	2019г
		1.3.2	Предлози за законски измени за дефинирање на обврски и надлежности во врска со КИИ.	ПЗ, 1.3.1	висок	МИОА	MKD-CIRT и сите останати засегнати страни	Буџет на РМ	2019г	2020г
		1.3.3	Предлози за минимални технички и организациски мерки за информациска безбедност за секој сектор.	ПЗ, 1.3.1	висок	ОТСБ*, МИОА	MKD-CIRT и сите останати засегнати страни	Буџет на РМ	2020г	2021г
		1.3.4	Усогласување и донесување секторски акти (материјални закони) со новиот закон за информациска безбедност	1.2, ПЗ, 1.3.1	висок	МИОА	Надлежни министерства	Буџет на РМ	2020г	2021г
		1.3.5	Усогласување на интерни акти на носители на КИИ	1.3.1, 1.3.4	висок	Носители на КИИ	Надлежни министерства	организациски и институционални буџети	2020г	континуирано
		1.3.6	Спроведување континуирана анализа, согледување на реалната состојба и дефинирање мерки и препораки за подигнување на нивото на сајбер безбедност во институциите надлежни за управување со КИИ и ВИС.	ПЗ, 1.3.1, 1.3.4, 1.3.5	висок	ОТСБ*	MKD-CIRT, надлежни министерства, универзитети, носители на КИИ и ВИС	Буџет на РМ	2020г	2022г

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
		1.3.7	Континуирано подобрување на отпорноста, интегритетот и доверливоста на КИИ и ВИС.	П3, 1.3.6	висок	НССБ, ОТСБ*	надлежни министерства, универзитети, носители на КИИ и ВИС	Буџет на РМ	2020г	2022г
		1.3.8	Дефинирање прецизни процедури за чување и заштита на податоци кои се процесираат во системите на КИИ и ВИС и спроведување континуирана анализа и ревизија на ефикасноста на дефинираните процедури.	П2, П3, 1.3.1	висок	ОТСБ*	MKD-CIRT, ДЗЛП, надлежни министерства, носители на КИИ и ВИС	Буџет на РМ	2020	2022г
		1.3.9	Спроведување на редовни ревизии со цел детектирање на грешки и ранливости на информациските системи и мрежи кои се дел од КИИ и ВИС.	П2, П3	висок	ОТСБ*	MKD-CIRT, надлежни министерства, универзитети, носители на КИИ и ВИС	Буџет на РМ	2020	2022г
		1.3.10	Развој и периодично тестирање на планови/сценарија за сајбер одбрана од сајбер напади	П2, П3	висок	ОТСБ*	сите конституенти на национална одбрана	Буџет на РМ	2020	2022г
1.4	Користење најдобри решенија за превенција и одговор на сајбер инциденти со цел заштита на националните безбедносни интереси.	1.4.1	Следење на најновите закани врз сајбер безбедноста	П2	висок	MKD-CIRT, ОТСБ*	сите засегнати страни	Буџет на РМ	2019	континуирано
		1.4.2	Следење и имплементација на најновите и најдобри хардверски и софтверски решенија како одговор на сајбер инциденти.	П2	висок	ОТСБ*	сите засегнати страни	Буџет на РМ	2020	континуирано
		1.4.3	Континуирано унапредување на технолошките и организациските мерки за ефикасно справување со сајбер заканите.	П2	висок	MKD-CIRT, ОТСБ*	сите засегнати страни	Буџет на РМ	2019	континуирано
		1.4.4	Развој на методологија за процена на ризици од сајбер закани на национално ниво.	П1	висок	НССБ	MKD-CIRT, сите засегнати страни	Буџет на РМ	2019г	2022г
		1.4.5	Континуирано следење, прифаќање и имплементација на меѓународно признати стандарди и процедури во областа на сајбер безбедноста.	П2	висок	НССБ	сите засегнати страни	Буџет на РМ	2019	континуирано
		1.5.1	Дефинирање на услови и одговорности во случај на кризна, вонредна и воена состојба во областа на сајбер безбедноста на национално ниво.	П4, 1.2.3	висок	ЦУК, МО, MKD-CIRT	ОТСБ*, надлежни министерства	Буџет на РМ	2019г	2020г
		1.5.2	Вклучување претставник за Сајбер безбедност во Управувачки комитет одговорен за предлагање мерки за постапување во кризна ситуација (ЦУК).	П5, 1.2.3	висок	ЦУК	НССБ	Буџет на РМ	2019г	2020г
1.6	Обезбедување /развој и имплементација на национални капацитети за редундантни оперативни и комуникациски	1.6.1	Идентификување на релевантни субјекти и анализа на надлежностите и координацијата на субјектите за водење критични операции во кризни/вонредни/воени состојби.	П2	висок	ОТСБ*	НССБ, надлежни министерства, MKD-CIRT	Буџет на РМ или донаторска	2020г	2021г
		1.6.2	Анализа на постоечките редундантни оперативни и комуникациски капацитети и интероперабилноста на комуникациско-информациските системи.							
		1.6.3	Реализација на проект за обезбедување на редундантни оперативни и комуникациски капацитети (изолирани од јавни комуникациски мрежи).							

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
	системи достапни во случај на сајбер инциденти од големи размери.	1.6.4	Донесување на процедури (стандардни, оперативни и безбедносни) за воспоставување на комуникациски протоколи помеѓу релевантни субјекти за справување со кризни/вонредни/воени состојби.					помош		
		1.6.5	Спроведување на редовни обуки и вежби за редундантните оперативни и комуникациски протоколи, прилагодени на улогите и надлежностите на секој субјект во планот за справување со кризни/вонредни/воени состојби.				ЦУК, MKD-CIRT, надлежни министерства, универзитети			

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
ЦЕЛ 2: САЈБЕР КАПАЦИТЕТИ И КУЛТУРА ЗА САЈБЕР БЕЗБЕДНОСТ										
2.1	Формирање на Институт за сајбер безбедност и дигитална форензика	2.1.1	Формирање на Национален институт за сајбер безбедност во соработка со сите универзитетски единици што имаат капацитети во областа на сајбер безбедноста.		висок	МО/Воена академија	Универзитети	Буџет на РМ	2019г	континуирано
		2.1.2	Формирање на Регионален центар за сајбер безбедност	2.1.1	висок	ОТСБ*, ИСБДФ	ФИТР, MKD-CIRT, МНР, МИОА, МО, МВР, регионална соработка WB6, Универзитети,	Донаторска помош	2020г	континуирано
		2.1.3	Имплементација на Центар за извонредност за сајбер безбедност како модел за зајакнување на капацитетите		висок	ОТСБ*, ИСБДФ	ФИТР, MKD-CIRT Универзитети	Донаторска помош	2021	континуирано
2.2	Развој и промовирање на наставни програми и обуки во областа на сајбер безбедноста на сите нивоа на образование.	2.2.1	Усовршување на постоечките и развој на нови наставни програми во основните и средните училишта и вклучување на елементи од областа на сајбер безбедноста во новите универзитетски студиски програми.	2.1.1	висок	МОН	ИСБДФ, Универзитети, АКВО, БРО	Буџет на РМ	2019г	континуирано
		2.2.2	Едуцирање и обука на наставниот персонал во основните и средните училишта во областа на сајбер безбедноста и обезбедување соодветни и современи материјали за учениците.	2.1.1	висок	МОН	ИСБДФ, АКВО, БРО, Универзитети	Буџет на РМ	2019г	континуирано
2.3	Зголемување на свеста и основните познавања во областа на сајбер безбедноста кај граѓаните со вклучување и соработка на сите релевантни засегнати страни.	2.3.1	Развој и дистрибуција на едукативни материјали по целни групи.	П2, 2.1.1	среден	ОТСБ*	МИОА, MKD-CIRT, НБРМ, АЕК, МВР, универзитети, сите засегнати страни	Буџет на РМ	2019г	континуирано
		2.3.2	Креирање платформа за електронско учење	П2	висок	ОТСБ*	МИОА, MKD-CIRT, ИСБДФ	Буџет на РМ	2020г	континуирано
		2.3.3	Поддршка на иницијативи, кампањи, конференции, работилници и семинари во областа на сајбер безбедноста наменети за поширокатa јавност.	П2, 2.1.1	среден	ОТСБ*, ИСБДФ	МИОА, MKD-CIRT, Универзитети	Буџет на РМ	2019г	континуирано
		2.3.4	Зголемување на свеста и основните познавања во областа на сајбер безбедноста на учениците во основните и средните училишта		среден	МОН	МИОА, MKD-CIRT, универзитети	Буџет на РМ	2019г	континуирано
2.4	Обезбедување едукација и обука и зголемување на свеста за сајбер безбедноста јавниот и приватниот сектор.	2.4.1	Обезбедување соодветна едукација и обука во областа на сајбер безбедноста за персоналот во јавната администрација.	П2, 1.6, 2.1	висок	ОТСБ*	ИСБДФ, МИОА, MKD-CIRT, Универзитети	Буџет на РМ	2019	континуирано
		2.4.2	Обезбедување соодветна едукација и обука во областа на сајбер безбедноста за менаџерски и раководен персонал во јавниот и приватниот сектор.	П2, 1.6, 2.1	среден	ОТСБ*	ИСБДФ, МИОА, MKD-CIRT, Приватен сектор, Универзитети	Буџет на РМ / Донаторска помош / организациски буџет	2019г	континуирано

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
		2.4.3	Зголемување на капацитетите за сајбер безбедност во малите и средните компании.	П2	среден	ОТСБ*	ИСБДФ, универзитети, МФ, МЕ, МИОА, MKD-CIRT, Д.З. За Статистика	Буџет на РМ / Донаторска помош / организациски буџет	2019г	континуирано
2.5	Подобрување на капацитетите за сајбер безбедност на национално ниво	2.5.1	Обезбедување стручно-специјалистичко образование и обука за лицата кои работат во областа на сајбер безбедноста.		средно	сите засегнати страни		организациски и институционални буџети	2020г	2022г континуирано
		2.5.2	Воспоставување механизми за задржување на стручниот кадар од областа на ИКТ и сајбер безбедност.		средно	МИОА, МФ	сите засегнати страни	Буџет на РМ	2019	континуирано
		2.5.3	Поддршка на научно-истражувачките капацитети и бизнис иновации во полето на сајбер безбедноста	Р1, 2.1	средно	ФИТР	НССБ, ИСБДФ, Универзитети	Буџет на РМ	2019	континуирано
		2.5.4	Спроведување истражување и утврдување на националните приоритети и врз основа на тоа преземање активности и инвестиции за развој на сајбер безбедноста.	Р2	средно	ОТСБ*	ФИТР, ИСБДФ, сите засегнати страни	Буџет на РМ	2021г	2022г
		2.5.5	Зголемување на капацитетите за сајбер безбедност во носители на КИИ, ВИС и јавниот сектор.	Р2, Р3, 1.3.4, 1.3.5	средно	ОТСБ*, MKD-CIRT	ИСБДФ, МФ, МЕ, МИОА, Стопански комори	Буџет на РМ, Буџет на MKD-CIRT	2019	континуирано
2.6	Обезбедување насоки за реакција во случај на сајбер инциденти, сајбер криза на сите нивоа на општеството, вклучувајќи и насоки за однесување во секојдневните активности.	2.6.1	Насоки за развој на Планови за обнова по катастрофи на национално ниво.	1.3.1	висок	MKD-CIRT	ЦУК, ОТСБ*	Буџет на МКД-ЦИРТ	2019г	2020г
		2.6.2	Развој на Стратегијата за справување со напади на мрежен и апликациски слој, како и cloud напади		висок	MKD-CIRT	ЦУК, ОТСБ*	Буџет на МКД-ЦИРТ	2020г	2021г
2.7	Обезбедување и примена на најсоодветни хардверски и софтверски решенија за превенција, идентификација и управување со сајбер инциденти, во согласност со ИКТ стратегија.	2.7.1	Дефинирање критериуми и стандарди и креирање насоки за зголемување на безбедноста на хардверот и софтверот.	П2	средно	ОТСБ*	сите засегнати страни	Буџет на РМ	2019	2022
		2.7.2	Обезбедување на современи хардверски и софтверски решенија за превенција, идентификација и управување со сајбер напади.	П2, 2.7.1	средно	ОТСБ*	сите засегнати страни	Буџет на РМ	2019	континуирано
		2.7.3	Надзор над примената	П2		ОТСБ*	сите засегнати страни	Буџет на РМ		континуирано
2.8	Основање на центар за побезбеден интернет (ЦПИ)		Развивање на услуги во насока на подобрување на безбедноста на интернетот.		средно	Граѓански организации	МВР, други надлежни министерства, медиуми, бизнис сектор.	Донаторска помош	2019	континуирано

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
ЦЕЛ 3: СПРАВУВАЊЕ СО САЈБЕР КРИМИНАЛ										
3.1	Унапредување на капацитетите за справување со сајбер криминал.	3.1.1	Анализа на моменталните капацитети за справување со компјутерски криминал во РМ	П2	висок	МВР, ОТСБ*	MKD-CIRT, Останатите институции	Буџет на РМ / ЕУ фондови	2018г	2022г
		3.1.2	Идентификација на сите надлежни институции во РМ а кои имаат надлежност и капацитети за справување со компјутерски криминал							
		3.1.3	Изработка на Процедури и Препораки за соработка помеѓу сите институции вклучени во борбата против компјутерскиот криминал							
		3.1.4	Подготовка на студија за потребата од обуки за справување со комјутерски криминал и дигитална форензика на сите надлежни институции							
		3.1.5	Развивање на програми за обука и наставни програми на Национално ниво за справување со компјутерски криминал и дигитална форензика							
		3.1.6	Воспоставување на рамка за Соработка со приватниот сектор, интернет сервис провајдерите и кадемската заедница							
3.2	Хармонизација на националните со меѓународните политики поврзани со сајбер криминалот.	3.2.1	Анализа на моменталната методологија, процедури и соработка за справувањето со компјутерскиот криминал на национално ниво	П2, 3.1.1	висок	МВР, ОТСБ*	MKD-CIRT, Останатите институции	Буџет на РМ / ЕУ фондови	2018г	2022г
		3.2.2	Споредување на постоечките методологии и процедури со меѓународните политики за справување со компјутерскиот криминал и електронски докази	П2, 3.2.1						
		3.2.3	Предлог на нови или предлог промена на постоечките методологии и процедури за справување со компјутерск криминал и електронски докази	П2, 3.2.2						
3.3	Креирање единствена и сеопфатна правна рамка за сајбер криминал, земајќи ја предвид позитивната законска регулатива во РМ и ЕУ.	3.3.1	Анализа на моменталната законска рамка за компјутерски криминал	П2	висок	МВР, ОТСБ*	MKD-CIRT, Останатите институции	Буџет на РМ / ЕУ фондови	2018Г	2022Г
		3.3.2	Изработка на предлог за промени на правната рамка за компјутерски криминал и креирање на посебна дел кој ќе се однесува на компјутерски криминал и електронски докази согласно позитивната законска регулатива во ЕУ	П2, 3.2.1						
3.4	Модернизација на надлежните институции за ефикасна борба против сајбер криминал.	3.4.1	Анализа на моменталната состојба и идентификација на реалните потреби од опрема и ресурси на надлежните институции за ефикасна борба против сајбер криминал и дигитална форензика	П2	висок	МВР, ОТСБ*	Останатите институции	Буџет на РМ / ЕУ фондови	2018г	2022г
		3.4.2	Подготовка на план за набавка на потребната опрема и ресурси на институциите надлежни за справување со компјутерски криминал и дигитална форензика	П2, 3.4.1						
		3.4.3	Развој на способности и капацитети за дигитална форензика во други институции и ентитети со надлежности во полето на сајбер безбедност.	П2, 3.4.2						
		3.5.1	Воспоставување на систем/платформа за пријавување на компјутерски криминал и информации поврзани со кривични дела од областа на компјутерскиот криминал	П2						

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
3.5	Воспоставување ефикасни процедури за пријавување и истражување на сајбер криминал.	3.5.2	воспоставување на процедури за вклучување на приватниот сектор и академијата во процесот на обезбедување на информации поврзани со кривични дела од областа на компјутерскиот	П2	висок	МВР, ОТСБ*	MKD-CIRT, Останатите институции	Буџет на РМ / ЕУ фондови	2018г	2022г
		3.5.3	Воспоставување на процедури за размена на добиените информации од ситемот со сите институции кои имаат надлежност во областа на справување со компјутерскиот криминал	П2						
3.6	Воспоставување формални механизми и процедури за соработка и размена на информации во областа на сајбер криминалот помеѓу релевантните национални субјекти и другите безбедносни служби.	3.6.1	Подготовка на судија за потребата за соработка и рамките на соработка помежу институциите		висок	МВР, ОТСБ*	MKD-CIRT, Останатите институции	Буџет на РМ / ЕУ фондови	2018г	2022г
		3.6.2	Подготовка на Процедури за соработка и размена на информации помеѓу релевантните национални субјекти и другите безбедносни служби							
		3.6.3	Подготовка и воспоставување на конкретни процедури за соработка помеѓу Секторот за компјутерски криминал и дигитална форензика (МВР) и МКД-ЦИРТ							
3.7	Унапредување на соработката со регионалните и меѓународните организации за борба против сајбер криминалот.	3.7.1	Анализа на моменталната состојба во однос на соработката со регионалните и меѓународните организации за справување со компјутерски криминал		висок	МВР, ОТСБ*	MKD-CIRT, Останатите институции	Буџет на РМ / ЕУ фондови	2018г	2022г
		3.7.2	Воспоставување на нови механизми и развивање на процедури за соработка со регионалните и меѓународните организации за борба против компјутерски криминал.							
		3.7.3	Развивање на процедури на Национално ниво за соработка со меѓународните интернет сервис провајдери							
		3.7.4	Воспоставување на процедури за учество на другите институции со надлежност за справување со копјутерски криминал во соработката на регионално и меѓународно ниво							
3.8	Унапредување на постоечките и воспоставување на нови механизми за соработка и размена на информации со приватниот и граѓанскиот сектор.	3.8.1	Анализа на ефикасноста на постоечките механизми за соработка со MKD-CIRT, приватниот и граѓанскиот сектор.		висок	МВР, ОТСБ*	MKD-CIRT, Останатите институции	Буџет на РМ / ЕУ фондови	2018г	2022г
		3.8.2	Студија и идентификација на реалната потреба за соработка на јавниот, приватниот и граѓанскиот сектор и дефинирање на рамка за соработка.							
3.9	Обезбедување стручно-специјалистичко образование и обука за лицата кои работат во областа на идентификација и истражување на сајбер криминал.	3.9.1	Идентификација на постоечките и релевантните стручно специјалистичко образование и обуки на Национално и Меѓународно ниво		висок	МВР, ОТСБ*	Останатите институции	Буџет на РМ / ЕУ фондови	2018г	2022г
		3.9.2	Изработка на план и процедури за учество на стручно специјалистички обуки на национално и меѓународно ниво на преставници од сите институции кои имаат надлежност за справување со компјутерски криминал							
3.10	Креирање мултидисциплинарна академска средина за унапредување на националните капацитети за истражување на сајбер криминалот.	3.10.1	Анализа на моменталните ресурси и капацитети за академски истражувања поврзани со компјутерскиот криминал и дигиталната форензика		висок	МВР, ОТСБ*	MKD-CIRT, Останатите институции	Буџет на РМ / ЕУ фондови	2018г	2022г
		3.10.2	Креирање на Центарот за инвороднот за компјутерска безбедност							
		3.10.3	Воспоставување на процедури за учество во истражувачките активности на Центарот за инзвороднот од аспект на справување со компјутерски криминал и дигитална форензика							

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
3.11	Активно учество во креирањето на меѓународни регулативи и стандарди за сајбер криминал и нивно имплементирање на национално ниво.	3.11.1	Активно следење на сите нови Регулативи, стандарди, директиви и препораки на меѓународно ниво за справување со компјутерски криминал и дигитална		среден	МВР, ОТСБ*	Останатите институции	Буџет на РМ / ЕУ фондови	2018	2022
		3.11.2	Изработка на план за имплементација на сите Регулативи, стандарди, директиви и препораки на меѓународно ниво за справување со компјутерски криминал и дигитална форензика, вклучувајќи ги сите институции надлежни за справување со компјутерски криминал							
3.12	Континуирана процена на соодветноста и ефективноста на националната регулатива за сајбер криминал.	3.12.1	Анализа и проценка на соодветноста и ефикасноста на постоечката законска регулатива за справување со компјутерскиот криминал		среден	МВР, ОТСБ*	Останатите институции	Буџет на РМ / ЕУ фондови	2018	2022
		3.12.2	Изработка на предлози за дополнување и промена на националната законска регулатава во делот на идентификација и истражување на компјутерскиот криминал							
3.13	Континуирана едукација на правосудните органи во областа на сајбер безбедност, сајбер криминал и електронски докази.	3.13.1	Анализа на потребите за едукација и обука на правосудните органи во областа на истражување на компјутерскиот криминал и електронските докази		висок	МВР, АСЈО	МП, ЈО	Буџет на РМ / ЕУ фондови	2018	2022
		3.13.2	Подготовка на Наставна програма за правосудните органи							
		3.13.3	Подготовка на План за спроведување на едукација и обука на правосудните органи за истражување на компјутерскиот криминал и електонски докази.							

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
ЦЕЛ 4: САЈБЕР ОДБРАНА										
4.1	Дефинирање на националните капацитети за сајбер одбрана.	4.1.1	Обезбедување ефикасен систем за заштита на класифицираните информации во сајбер просторот преку континуирано унапредување на степенот на заштита од сајбер напади и сајбер шпионажа на националните системи и мрежи низ кои се процесираат класифицирани информации.	Закон за класифицирани информации	висок	ДБКИ	сите конституенти	буџет	тековно	тековно
		4.1.2	Изработка на стратегија за сајбер одбрана	Национална стратегија за сајбер безбедност	висок	МО	АРМ, МВР, ДБКИ, ЦУК, АР, МИОА, ДЗС, MKD-CIRT	буџет	01.11.2018	31.03.2019
		4.1.3	Развој на национални полиси, процедури и инструкции од полето на сајбер одбрана	4.1.2	висок	МО	АРМ, МВР, ДБКИ, ЦУК, АР, МИОА, ДЗС, MKD-CIRT	буџет	01.05.2019	31.12.2020
		4.1.4	Развој на способности и капацитети за сајбер одбрана кај сите конституенти што се дел од националната одбрана	Национална стратегија за сајбер безбедност	висок	МО	MKD-CIRT, ОТСБ*	буџет/НАТО програми	тековно	тековно
		4.1.5	Дефинирање/Преглед на ресурси со кои располага државата, приватен и јавен сектор, во однос активна одбрана од сајбер напади	П2	висок	ОТСБ*, MKD-CIRT	сите државни институции, КИИ, ВИС, ИТ оператори, ИТ претпријатија од приватен и јавен сектор	буџет	6 месеци по формирање на Национално тело	1 години
		4.1.6	Дефинирање на критериуми за евалуација на сајбер одбранбените капацитети	П2, 1.2	висок	ОТСБ*	Конституенти на национална одрбана	буџет	3 месеци по донесување на регулатива	1 година
		4.1.7	Анализа на постеочката инфраструктура - институционалните капацитети, од техничко-технолошка и организациска смисла, за утврдување на капацитети со кои располага државата, а за потреби на сајбер одбраната. Да се утврдат слабостите и ризиците и да се најде начин за нивно подобрување односно унапредување.	4.1.6, П3	висок	ОТСБ*	МО, MKD-CIRT Конституенти на национална одрбана	буџет	3 месеци по дефинирање на 4.1.6	1 години
		4.2.1	Формирање и развој на воен CERT	4.1.2	висок	МО/АРМ	МО/АРМ	буџет/НАТО програми	6 месеци по 4.1.2	1 година
		4.2.2	Развој на способности и капацитети за сајбер одбрана во МО и АРМ	4.1.2	висок	МО/АРМ	МО/АРМ	буџет/НАТО програми	тековно	тековно

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
4.2	Дефинирање на воени капацитети во Министерството за одбрана и Армијата за справување со закани во сајбер просторот.	4.2.3	Развој на сајбер капацитети за предупредување, превенција, заштита, одвраќање, детекција, форензика и одбрана за воените КИС системи (стационарни и мобилни)	4.1.2	висок	МО/АРМ	МО/АРМ	буџет/НАТО програми	тековно	тековно
		4.2.4	Формирање и воспоставување на Воен авторитет за сајбер одбрана	4.1.2	висок	МО/АРМ	МО/АРМ	буџет	6 месеци по 4.1.2	1 година
		4.2.5	Користење на НАТО партнерство/членство за развој на ресурси, обуки, капацитети	прием во НАТО	висок	МО/АРМ	МО/АРМ	буџет	тековно	тековно
4.3	Формирање, развој и одржување на дефинираните капацитети и способности за сајбер одбрана.	4.3.1	Развој на CSIRC (Computer Security Incident Response Capability) за КИС на МО и АРМ	4.1.2	висок	МО/АРМ	МО/АРМ	буџет/НАТО програми	1 година по 4.1.2	2 години
		4.3.2	Развој на мобилни капацитети (CD-deploy) за сајбер одбрана компатибилен со НАТО КИС, на ниво на команда за баталјон	4.3.1	висок	МО/АРМ	МО/АРМ	буџет/НАТО програми	3 месеци по 4.3.1	2 години
		4.3.3	Развој на оперативни планови кај сите даватели на услуги во сајбер просторот согласно националните сценарија	4.1.7	среден	ОТСБ*, MKD-CIRT	сите даватели на услуги во сајбер простор	буџет	6 месеци по дефинирање на 4.1.7	2 години
4.4	Креирање единствена и сеопфатна правна рамка за сајбер одбрана, земајќи ја предвид позитивната законска регулатива во РМ и директивите од НАТО и ЕУ.	4.4.1	Усогласување регулативите за сајбер одбрана, согласно позитивната законска регулатива во РМ и директивите од НАТО и ЕУ.	4.1.2	висок	МО/АРМ	МП, СЗ	буџет	тековно	тековно
		4.4.2	Дефинирање и имплементација на мерки за стратешко раководење со сајбер одбраната	Национална стратегија за сајбер безбедност	висок	ОТСБ*	сите конституенти на националната одбрана	буџет	тековно	тековно
4.5	Одбрана и намалување на ризиците во сајбер просторот.	4.5.1	Развој на методологија за процена на ризици од сајбер закани на ниво на МО и АРМ.	4.1.2	висок	МО/АРМ	ССВБиР	буџет	6 месеци по 4.1.2	2 години
		4.5.2	Континуирана заштита на доверливост, интегритет и автентикација на податоците и информациите за воените мрежи (КИС)	континуирано	висок	МО/АРМ	ДБКИ	буџет	тековно	тековно
4.6	Воспоставување и одржување на взаемна меѓународна соработка за одвраќање на споделените сајбер закани и зголемување на националната и меѓународната безбедност и стабилност.	4.6.1	Дефинирање на национална точка за контакт за НАТО сајбер операции и соработка	прием во НАТО	висок	МО/АРМ	МО/АРМ	буџет	прием во НАТО	6 месеци
		4.6.2	Воспоставување на точка за безбедна комуникација, за потреби на националните авторитети со НАТО, преку обезбедување на интероперабилност и усогласеност со НАТО криптографски систем (специјални документи за криптографски систем) за заштита на доверливост, интегритетот и автентикација на овие податоци и информации	Програма за реформи	висок	МО	АРМ, ДБКИ	буџет	12.2018	04.2020
		4.6.3	Вклучување на РМ во колективната сајбер одбрана на НАТО и искористување на ресурсите	прием во НАТО	висок	МО	АРМ	буџет	прием во НАТО	тековно
4.7	Дефинирање и координација на военото планирање за начинот и употребата на воените сајбер капацитети со националната сајбер одбрана во разни ситуации.	4.7.1	Дефинирање регулативи за начинот на употребата на воените сајбер капацитети во процесот на националната сајбер одбрана во разни ситуации.	4.1.2	висок	МО/АРМ	МО/АРМ	буџет	3 месеци по 4.1.2	2 години
		4.7.2	Вклучување на експерти од МО и АРМ во националните тела за справување (управување) со сајбер закани	П2,формирање на Национални тела	висок	ОТСБ*	МО/АРМ	буџет	тековно	тековно
4.8	Вклучување и придонес во колективната сајбер одбрана преку меѓународна соработка.	4.8.1	Формирање на систем за интероперативност и усогласеност на националните криптографски систем (специјални документи за криптографски систем)со криптографски систем на НАТО за заштита на доверливост, интегритетот и достапност на овие податоци и информации	прием во НАТО	висок	МО	АРМ	буџет	прием во НАТО	тековно

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
		4.8.2	Следење и имплементација на НАТО стандарди и насоки од областа на сајбер безбедноста/одбраната	прием во НАТО	висок	МО	АРМ	буџет	тековно	тековно
4.9	Континуирана едукација за обезбедување на високо ниво на свесност и лична одговорност во однос на сајбер одбраната и националната одбрана и безбедност.	4.9.1	Обука и подигнување на свест за сајбер одбрана преку едукација и тренинг на целиот персонал во МО и АРМ	4.1.2	висок	МО/АРМ	Воена Академија	буџет	тековно	тековно
		4.9.2	Дефинирање и континуирано едуцирање на потребен број на експерти за оперативна и тактичка сајбер одбрана и управување со сајбер опасностите во КИС	4.1.2	висок	МО/АРМ	Воена Академија	буџет	тековно	тековно
		4.9.3	Организација на национални вежби за сајбер одбрана во соработка со сите чинители кои се дел од сајбер безбедноста	Национална стратегија за сајбер безбедност	висок	MKD-CIRT	МО, ОТСБ*, МИОА Конституенти на национална одбрана	буџет на РМ, буџет НаMKD-CIRT, донации	тековно	тековно
		4.9.4	Подигнување на свесност за закани и ризици во сајбер просторот за потребите на националната одбрана	Национална стратегија за сајбер безбедност, П2, 4.1.2	висок	ОТСБ*	Конституенти на националната одбрана	буџет	тековно	тековно
		4.9.5	Интеграција на сајбер одбраната во сите оперативни вежби на национално ниво	Национална стратегија за сајбер безбедност, П2	висок	МО, ОТСБ*, MKD-CIRT	Конституенти на националната одбрана	буџет	тековно	тековно
4.10	Развој и имплементација на систем и програми за размена и споделување на информации, знаења и искуства меѓу јавниот, приватниот и одбранбено-безбедносниот сектор на полето на сајбер одбраната, со цел заштита на КИИ и ВИИ.	4.10.1	Активно учество на воени меѓународни вежби и семинари за сајбер одрбана	континуирано	среден	МО/АРМ	МО/АРМ	буџет	тековно	тековно
		4.10.2	Развој на цивилно воената соработка за потребите на сајбер одбрана со јавниот и приватен сектор	Национална стратегија за сајбер безбедност, П2	висок	ОТСБ*	јавен и приватен сектор, МО, АРМ	буџет	тековно	тековно
		4.10.3	Развој на систем и процедури за размена на информации за ризици и опасности во делот на сајбер одбраната на национално и меѓународно ниво	4.2.1	висок	MKD-CIRT	МО, АРМ, МИОА, ОТСБ*, оператори и авторитети на КИИ	буџет	тековно	тековно
		4.10.4	Воспоставување на соработка и размена на информации во националните системи за колективна одбрана во полето на сајбер одбраната	4.1.7	висок	ОТСБ*	сите конституенти на националната одбрана	буџет	4.1.7	тековно
		4.10.5	Воспоставување на систем за споделување на знаење и информации во областа на сајбер одбраната	2.1.1	среден	ИСБДФ	сите	буџет	тековно	тековно

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
ЦЕЛ 5: СОРАБОТКА И РАЗМЕНА НА ИНФОРМАЦИИ										
5.1	Промовирање на соработка на полето на сајбер безбедноста на национално ниво	5.1.1	Развој на ефективен модел за соработка на национално ниво помеѓу институциите кои имаат надлежност во областа на сајбер безбедноста и унапредување на нивната постоечка структура и процеси.	П2,П3	среден	ОТСБ*	сите засегнати страни	Буџет на РМ / Донаторска помош	2019г	2021
		5.1.2	Формирање регистер на национални експерти во Сајбер безбедност со тесна експертиза	П2	висок	MKD-CIRT	ОТСБ*	Буџет на РМ / Донаторска помош	2019г	2019
		5.1.3	Задолжување на сите институции од владиниот и јавниот сектор да станат конституенти на MKD-CIRT	П1, П2	висок	МИОА	МИОА, MKD-CIRT	Буџет на РМ / Донаторска помош	2019г	2019г
		5.1.4	Градење на мрежа од CIRT-ови во државата поврзани со националниот и меѓусебно		среден	MKD-CIRT	сите засегнати страни	Буџет на РМ / Донаторска помош	2019г	континуирано
		5.1.5	Ефикасна размена на информации помеѓу државата и субјектите кои управуваат со КИИ и ВИС	П2, 1.3.1	среден	ОТСБ*	MKD-CIRT, Носители на КИИ, сите засегнати страни	Буџет на РМ / Донаторска помош	2019г	континуирано
		5.1.6	Промовирање и унапредување на нормите, правилата и принципите на одговорно однесување од страна на државата, согласно утврдените принципи на меѓународно ниво.		среден	МИОА	сите засегнати страни	Буџет на РМ / Донаторска помош	2019	континуирано
		5.1.7	Соработка на засегнатите страни на истражувачки проекти на национално и меѓународно ниво.	П1	среден	НССБ	Академска заедница, сите засегнати страни	Буџет на РМ / Донаторска помош	2019	континуирано
		5.1.8	Соработка на сите засегнати страни за унифицирање безбедносни норми, стандардизирање на соработката и дефинирање и поставување задолжително ниво на заштита за субјектите кои управуваат со КИИ и ВИС.	П2, 1.3.1	среден	ОТСБ*	сите засегнати страни	Буџет на РМ / Донаторска помош	2019	континуирано
		5.1.9	Соработка со приватниот сектор за обезбедување сајбер простор кој нуди сигурна средина за размена на информации, истражување и развој и обезбедување безбедна информациска инфраструктура која ќе го стимулира претприемништвото со цел да ја поддржи конкурентноста на сите домашни компании и ќе ги заштити нивните инвестиции.	П1	висок	НССБ	МАСИТ, MKD-CIRT, МИОА, МЕ, КЗПВРМ за Економски прашања	Буџет на РМ / Донаторска помош	2019	континуирано
		5.1.10	Градење на доверба помеѓу сите засегнати страни, вклучувајќи и развој на национална платформа/систем за размена на информации во врска со закани, инциденти и непосредните опасности.	П1, 1.3.4, 1.3.5, 1.4.1, 1.4.2	среден	НССБ	MKD-CIRT	Буџет на РМ / Донаторска помош	2019	континуирано
		5.1.11	Соработка на засегнатите страни во насока на развој и имплементација на технологии кои ќе обезбедат максимална заштита и транспарентност, како и тестирање и процена на нивото на безбедност на искористените технологии.	П2, 1.3.8, 1.3.9, 1.4, 2.5.5, 2.6.1, 2.6.2, 2.7.1, 4.1	среден	ОТСБ*	МИОА,ИСБДФ, Универзитети	Буџет на РМ / Донаторска помош	2020	континуирано
		5.2.1	Воспоставување и унапредување на соработката и градење доверба со други меѓународни јавни и приватни CERT и CSIRT тимови, академски заедници и други меѓународни организации.		висок	MKD-CIRT		Буџет на РМ / Донаторска помош	2018	континуирано

Број на активност	Активност	Код	Начин на имплементација (Задачи)	предуслов	приоритет	Носител	Соработници	Финансирање	почеток	крај
5.2	Промовирање на соработка на полето на сајбер безбедноста на меѓународно ниво	5.2.2	Активно учество и давање придонес кон меѓународната способност за сајбер безбедност и јакнење на довербата.	П2	среден	ОТСБ*	сите други засегнати страни	Буџет на РМ / Донаторска помош	2019	континуирано
		5.2.3	Воспоставување механизми и процедури за меѓународна соработка на дипломатско ниво во случај на сајбер инциденти, напади и кризи, согласно утврдените принципи на меѓународно ниво.		среден	МНР		Буџет на РМ / Донаторска помош	2019	континуирано
5.3	Координиран пристап кон предизвикот за управување со Интернетот и норми на однесување	5.3.1	Соработка на сите засегнати страни за воспоставување национални, како и придонес во дефинирање на меѓународните легислативи поврзани со начинот на однесување во сајбер просторот, слободата на изразување, заштитата на личните податоци, правата на приватност и основните човекови права и слободи.		среден	МИОА	МП, ДЗЛП, народен правобранител, граѓански организации	Буџет на РМ / Донаторска помош	2019	континуирано
		5.3.2	Вклучување во соодветни ЕУ и меѓународни здруженија и програми за заштита на деца и млади од нелегални содржини, загрозување и активности кои постојат на интернет		висок	СЕП	сите засегнати страни	Буџет на РМ / Донаторска помош	2019	