Република Северна Македонија

Министерство за одбрана

Бр. 02-1249/1

12.02.2020 година

МИНИСТЕРКА ЗА ОДБРАНА

Радмила Шекеринска-Јанковска

СТРАТЕГИЈА ЗА

САЈБЕР ОДБРАНА

Содржина

Вовед

Безбедност на граѓаните, заштита на суверенитетот и територијалниот интегритет, принципи на демократијата и владеењето на правото се едни од главните концепти и основни принципи на модерното демократско општество на Република Северна Македонија. За да ги одржи овие вредности, државата мора да изгради и да одржува комплексен систем на национална одбрана заснован на долгорочни визии и стратегии. Социјалните и технолошките достигнувања во општеството доведоа до потреба од промени во конвенционалните форми и методи применети во областа на одбраната. Сајбер нападите стануваат сè пософистицирани и поштетни. Воедно, новиот хибриден начин на војување се базира на асиметрични воени методи и многу активности кои се одвиваат во сајбер просторот, што е причина сајбер просторот сè почесто да се дефинира како петта димензија на војување.

НАТО го признава сајбер просторот како планирачки и оперативен домен, а сајбер нападот како потенцијален активатор на член 5 од северно-атлантскиот договор. Затоа, во согласност со условите од член 3 од северно-атлантскиот договор, земјите треба да ги одржуваат и развиваат индивидуалнитеи колективните капацитети, со цел да се справат со предизвиците и заканите во сајбер просторот. Република Северна Македонија е посветена на зголемување на националните способности, но и градење на колективни способности преку учество во заеднички активности и интензивирање на соработката во областа на сајбер одбраната на регионално и меѓународно ниво.

Во таа насока Република Северна Македонија во јули 2018 ја донесе Националната стратегија за сајбер безбедност, а во декември 2018 Акцискиот план за имплементација на стратегијата и започна со имплементација на дефинираните активности. Националната стратегија за сајбер безбедност ја препознава сајбер одбраната како автономна и специфична гранка во поширокиот концепт на сајбер безбедноста. Исто така, согласно Законот за одбрана, сајбер одбраната се перципира како дел од одбраната на државата. Законот ја дефинира одбраната на државата како систем за одбрана на независноста и територијалниот интегритет,

како и заштита на животите на граѓаните и нивниот имот од надворешен напад. Ова вклучува изградба на ефикасен систем на национална одбрана, подготовка и ангажирање на релевантни сили и средства и учество во колективниот одбранбен систем на НАТО.

Сајбер одбраната се разликува од сајбер безбедноста главно во природата и интензитетот на сајбер нападите, без постоење можност да се дефинираат точни критериуми. Затоа, подготвеноста за одбрана од сајбер напади мора да биде комплексна и не смее да се фокусира само на полето за безбедноста. Државата мора да развие сопствени капацитети и способности за да се спротивстави дури и на такви сајбер напади кои што би можеле да ја активираат одбраната на државата. Специфична карактеристика на сајбер одбраната ќе биде фактот дека таа ќе биде активна не само во итни и кризни состојби, туку ќе делува постојано и во секојдневни ситуации.

Камен-темелник за развој на ефикасен систем за сајбер одбрана во Република Северна Македонија е заложбата на Владата за градење на капацитети и зајакнување на сајбер одбраната, зацртана и во Акцискиот план за сајбер безбедност на Република Северна Македонија 2018-2022. Концептот е базиран на свесно разбирање на разликите помеѓу сајбер безбедноста и сајбер одбраната. Во оваа Стратегија за сајбер одбрана се дефинираат концептуалните услови за соодветна одбрана на Министерството за одбрана на Република Северна Македонија и Армијата на Република Северна Македонија (Армија) во сајбер просторот и се претставени основната визија, мисија и целите, опишувајќи ја планираната крајна состојба на поединечни области на проблемот. Активностите произлегуваат од одбранбената определба на Република Северна Македонија, ги рефлектираат актуелните трендови на современите одбранбени доктрини и се во целосна согласност со основните правила на една демократска држава. Со подготовка и реализирање на овие активности се одржуваат и заштитуваат основните права и слободи на поединците, како и горенаведените принципи и вредности, бидејќи безбедноста и слободата не се контрадикторни една со друга. Не постои слобода без безбедност, ниту пак безбедност без слобода.

Стратегија за сајбер одбрана е развиена во согласност со Националната стратегија за сајбер безбедност, Стратегијата за сајбер безбедност на Европската унија и Политиката и заложбата за сајбер безбедност на НАТО за обезбедување на сигурно, безбедно, доверливо и отпорно дигитално опкружување.

Клучни предизвици за сајбер одбраната на Република Северна Македонија

Постојат голем број потенцијални напаѓачи, државни или недржавни актери, кои можат да извршат сајбер напад со интензитет што може да го активира системот за сајбер одбрана на Република Северна Македонија. Сајбер нападите се идеални алатки за нанесување штета на политички, деловни или други цели, како и силна алатка за спроведување на намерите на напаѓачите. Во исто време, најчесто е многу тешко да се идентификува напаѓачот, со што се намалува можноста од потенцијален соодветен одговор на нападот. Овие факти, заедно со отсуството на географски и слични ограничувања, кои ја намалуваат можноста за откривање на локацијата и идентификување на напаѓачите, се основа за сè поголема искористеност на сајбер просторот за реализирање на злонамерни активности од различни побуди и кон различни цели.

Примарни цели на сајбер нападите можат да бидат корисниците и системите кои тесно ја поврзуваат компјутерската средина со физичката инфраструктура. Нападите можат дури и директно да бидат насочени кон компоненти на одбранбената инфраструктура.

Еден од клучните предизвици со кој се соочува сајбер одбраната е напредокот на офанзивните сајбер способности на потенцијалните непријателски држави. Други предизвици се сè поголемата употреба на сајбер просторот од страна на терористи и терористички организации, растечкиот тренд на злоупотреба на сајбер просторот од страна на криминалците и криминалните организации, како и взаемната поврзаност на државни и недржавни напаѓачи.

Растечката зависност на функционалноста на безбедносните и одбранбените сили на државата од информатичките и комуникациските технологии ја зголемува потребата од воспоставување функионален систем за сајбер одбрана. Како подоминантни воочени слабости и предизвици можат да се издвојат недостатокот на безбедносни политики, процедури и инструкции, ниската дигитална писменост

и недоволната свест на индивидуалните корисници за безбедносните правила кои треба да се почитуваат во сајбер просторот.

Најважните предизвици, трендови и потенцијалните закани врз македонското општество, а воедно и врз одбранбениот систем на Република Северна Македонија, се дефинирани во Националната стратегија за сајбер безбедност.[1]

[1]Национална стратегија за сајбер безбедност 2018-2022, http://www.mio.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_sajber_bezbednost_2018-2022.pdf

Визија и Мисија

Визија

Визијата на Стратегијата за сајбер одбрана, согласно Националната стратегија за сајбер безбедност, е да се создаде и одржува сигурно, безбедно, доверливо и отпорно дигитално опкружување, поддржано од квалитетно изградени способности и капацитети, високо квалификувани експерти, изградено ниво на доверба и национална и меѓународна соработка во областа на сајбер одбраната.

Мисија

Мисијата на Стратегијата за сајбер одбрана е да се развијат и зајакнат капацитетите и способностите за активно следење на сајбер просторот од заканите и нападите и намалување на ефектите од овие закани, со цел заштита на националните интереси.

Стратегиски цели

Стратегијата за сајбер одбрана се заснова на остварување на четири стратешки цели чија основна цел е зајакнување на капацитетите за следење и одбрана од сајбер закани и напади и зголемување на безбедноста во сајбер просторот во сите сектори и на сите нивоа.

Слика 1: Цели на Стратегијата за сајбер одбрана

1. СПОСОБНОСТИ ЗА САЈБЕР ОДБРАНА

Воспоставување и одржување соодветни способности за сајбер одбрана со основна цел заштита на националните интереси

Со цел да се заштити сајбер просторот, од клучно значење е да се развијат адекватни способности за сајбер одбрана. Овие способности треба да обезбедат основа за успешни сајбер операции поврзани со одбрана на сајбер просторот, како во Министерството за одбрана на Република Северна Македонија и Армијата, така и на национално и меѓународно ниво. Министерството за одбрана на Република Северна Македонија и Армијата ќе развијат капацитети и способности, кои ќе дадат свој активен придонес во сајбер одбраната во државата и ќе бидат поддршка на меѓународните организации (ООН, НАТО и ЕУ и др.) за справување со заканите на глобално ниво. Способностите кои ќе се развијат ќе имаат можност проактивно да предвидат опасности од потенцијални напади, да лоцираат активни сајбер напади, како и да анализираат и да практикуваат можни одговори за заштита од истите, преку градење на способности за сајбер отпорност и сајбер одвраќање. Исто така, ќе се развијат способности за активно и успешно менаџирање со кризи со кои би се соочиле во случај на потенцијални успешни сајбер напади. За исполнување на оваа цел еден од клучните предизвици е соочувањето со недостиг од квалификуван и добро обучен персонал за сајбер одбрана. Оттука, еден од главните проритети ќе биде поефикасно регрутирање на соодветен кадар, како и задржување и мотивирање на постоечкиот.

1.1. Национални способности за сајбер одбрана

1.1.1 Развој на соодветни способности и ефикасни капацитети за сајбер одбрана кај сите конституенти што се дел од националната одбрана.

1.1.2 Дефинирање на критериуми за евалуација на сајбер одбранбените капацитети и способности.

1.1.3 Анализа, евиденција и евалуација на постоечката инфраструктура и институционалните капацитети со кои располага државата, јавниот и

приватниот сектор, а кои можат да се искористат за потребите на сајбер одбраната.

1.1.4 Изработка и имплементација на мерки за стратешко раководење со националните капацитети за сајбер одбрана согласно Законот за одбрана и други поврзани национални регулативи.

1.2. Воени способности во Министерството за одбрана на Република Северна Македонија и Армијата за справување со закани во сајбер просторот

1.2.1 Формирање и развој на Воен тим за следење, координација и справување со компјутерски инциденти (MIL-CIRT).

1.2.2 Развој на способности и капацитети за сајбер одбрана во Министерството за одбрана на Република Северна Македонија и Армијата.

1.2.3 Формирање и воспоставување на Воен авторитет за сајбер одбрана.

1.2.4 Континуирано обезбедување на доверливост, интегритет и достапност на податоците и информациите за воените мрежи и системи.

1.2.5 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 системите и мрежите на Министерството за одбрана на Република Северна Македонија и Армијата низ кои се процесираат класифицирани информации

1.2.6 Развој на распоредливи капацитети за сајбер одбрана компатибилни со НАТО на рамниште на команда на баталјон.

1.2.7 Идентификација на потребите за сајбер професионалци и дефинирање на базен на потенцијални човечки ресурси.

1.2.8 Развивање мотивирачки систем на награди и унапредувања на стручниот персонал од областа на сајбер безбедноста и одбраната, заснован на квалитетот и покажаните резултати на кадарот преку определување додаток на плата на стручниот персонал од областа на сајбер безбедноста и одбраната, во зависност од работните задачи, стручноста и незаменливоста.

1.2.9 Формирање на активна резерва за потребите на сајбер одбраната и соодветно дефинирање на политики за регрутација и ангажман на стручни лица од оваа област.

1.2.10 Воспоставување програми за размена на искуства со експерти од цивилни компании со цел подобрување на обученоста на кадарот за сајбер одбрана

2. ЕДУКАЦИЈА И ОБУКА

Градење високо квалитетен и обучен клучен персонал за сајбер одбрана, како и одржување на основните принципи за сајбер хигиена преку константна основна обука на вработените

Оваа стратешка цел се фокусира на градење способности кои ќе овозможат засегнатите страни да се стекнат со соодветно ниво на знаење во областа на сајбер одбраната. Промовирањето на сајбер хигиена и зголемување на свесноста за сајбер безбедност значи поттикнување на одговорност и разбирање за сајбер ризиците во сите сфери на општеството, притоа давајќи на знаење дека заштитата на личните податоци најчесто е обврска на секој поединец, а потоа и на различните провајдери на услуги. Постигнувањето на оваа цел значи креирање вештини, знаења и искуства за заштита, притоа обезбедувајќи поголема отпорност од злонамерни сајбер активности.

Во процесот на стекнување на вештини, знаења и искуства во областа на сајбер безбедноста на национално ниво значајна улога ќе имаат и формирањето на Институт за сајбер безбедност и дигитална форензика во рамките на Воената академија „Генерал Михаило Апостолски“ - Скопје, формирање на ад-хок меѓуресорски истражувачки тимови составени од експерти од јавниот сектор, приватниот сектор и академската заедница, како и активното учество на различни истражувачки и вежбовни активности организирани од страна на партнерски држави и меѓународни организации.

2.1. Континуирана едукација за обезбедување на високо ниво на свесност и лична одговорност во однос на сајбер одбраната во контекст на националната одбрана и безбедност

2.1.1 Подигнување на свеста за сајбер одбрана преку едукација и обука на целокупниот персонал во Министерството за одбрана на Република Северна Македонија и Армијата.

2.1.2 Дефинирање и континуирано едуцирање на потребен број на експерти за стратегиска, оперативна и тактичка сајбер одбрана и за менаџмент со сајбер заканите во Министерството за одбрана на Република Северна Македонија и Армијата.

2.1.3 Формирање и воспоставување на Институт за Сајбер безбедност и дигитална форензика во рамките на Воената академија, со основна цел истражување, едукација и обука во делот на сајбер одбраната.

2.1.4 Активно учество во НАТО кооперативниот центар за извонредност за сајбер одбрана (CCDCOE) со испраќање на национални експерти и учество во истражувачките активности на Центарот.

2.1.5 Креирање и развој на симулациски сценарија и програми за сајбер безбедносни инциденти што ќе се користат во националните вежби за сајбер одбрана.

2.1.6 Организација на национални вежби за сајбер одбрана во соработка со сите чинители што се дел од системот за националната одбрана.

2.1.7 Интеграција на сегментот на сајбер одбраната во сите оперативни вежби на национално ниво, во делот за национална одбрана.

2.1.8 Активно учество на меѓународни воени вежби и обуки за сајбер одбрана.

2.1.9 Заедничкото споделување на капацитети и искуства со НАТО, ЕУ и партнерски држави.

3. СОРАБОТКА И РАЗМЕНА НА ИНФОРМАЦИИ

Унапредување на соработката и размената на информации на национално и меѓународно ниво

Изолираноста на една држава во справување со сајбер закани е предодредена на неуспех. Ефикасна сајбер одбрана може да се постигне само во соработка со државни и недржавни ентитети, како на национално, така и на меѓународно ниво. За таа цел е потребно да се дефинираат соодветни процеси, процедури и протоколи за соработка и размена на информации помеѓу засегнатите страни. Сајбер просторот претставува комплексна димензија каде е тешко да се дефинираат границите. Затоа освен потребата од ефикасна соработка на национално ниво, има потреба од воспоставување на силни регионални, како и меѓународни сојузи, главно во рамките на ООН, НАТО, ЕУ. Во рамките на напорите за соработка, од суштинско значење ќе биде подготовката и учеството во различни вежбовни активности организирани од меѓународните организации, бидејќи тие претставуваат важен извор на информации и размена на искуства во врска со техничките и правните димензии за уредување на сајбер одбраната. Исполнувањето на оваа стратешка цел ќе донесе значително подобрување на сајбер одбраната, не само на Република Северна Македонија, туку и на сојузничките земји и организации.

3.1 Воспоставување и одржување на взаемна меѓународна соработка и размена на податоци за одвраќање на споделените сајбер закани и зголемување на националната, регионалната и меѓународната безбедност и стабилност

3.1.1 Развој и имплементација на систем и програма 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.

3.1.2 Развој на цивилно-воена соработка за потребите на сајбер одбраната и промовирање на соработка помеѓу јавниот и приватниот сектор.

3.1.3 Воспоставување на соработка и размена на информации од доменот на сајбер одбрана помеѓу сите конституенти на системот за национална одбрана.

3.1.4 Дефинирање на национална точка за контакт со НАТО во поглед на сајбер операции и соработка.

3.1.5 Воспоставување на точка за безбедна комуникација со НАТО.

3.1.6 Вклучување на Република Северна Македонија во колективната сајбер одбрана на НАТО и воспоставување на систем за соработка и размена на информации.

3.1.7 Воспоставување и одржување на соработка со други партнерски држави во областа на сајбер одбраната

4. ПРАВНА И РЕГУЛАТОРНА РАМКА

Усогласување на постоечките и имплементирање нови соодветни законски регулативи, прописи и процедури за одбрана на сајбер просторот и заштита на националните интереси

Република Северна Македонија на крајот на 2018 година ја усвои Националната стратегија за сајбер безбедност, поради што уредувањето на сајбер одбраната и јакнењето на сите останати капацитети поврзани со сајбер одбраната се на самиот почеток. Од таа причина, регулативите, прописите и процедурите поврзани со сајбер одбраната, а воедно и со сите останати сегменти на сајбер безбедноста, не се дефинирани во целост. Во оваа фаза, потребно е да се користат постоечките законски регулативи и да се дефинираат основните компетенции и овластувања на засегнатите страни, како и правата и обврските на лицата кои ги вршат горенаведените овластувања во областа на сајбер безбедноста и одбраната. Многу важен сегмент е и дефинирањето и воспоставувањето на ефикасен систем за контрола на активностите поврзани со уредување на сајбер одбраната. Дополнително, ќе се дефинираат и донесат дополнителни правни акти за да се создаде законска рамка согласно националните потреби, како и согласно насоките од меѓународните организации. Исполнувањето на оваа стратешка цел ќе ги дефинира основните правни аспекти на сајбер одбраната. Важен чекор ќе биде нашето учество во правната регулација на сајбер одбраната на меѓународно ниво.

4.1. Креирање единствена и сеопфатна правна рамка за сајбер одбрана, земајќи ја предвид позитивната законска регулатива во Република Северна Македонија и директивите од НАТО и ЕУ

4.1.1 Развој и имплементација на систем и програма 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 ККИИ и ВКИИ.

4.1.2 Развој на нови и усогласување на постоечките регулативи за сајбер безбедност и одбрана, согласно позитивната законска регулатива во Република Северна Македонија и директивите од НАТО и ЕУ.

4.1.3 Дефинирање и имплементација на мерки за стратешко раководење со сајбер одбраната во Министерството за одбрана на Република Северна Македонија и Армијата

4.1.4 Развој на методологија за процена на ризици од сајбер закани на ниво на Министерството за одбрана на Република Северна Македонија и Армијата

4.1.5 Развој на оперативни планови кај сите даватели на услуги во сајбер просторот согласно планот за одбрана.

4.1.6 Развој на систем и процедури за размена на информации за заканите и ризиците во полето на сајбер одбраната на меѓународно ниво.

4.1.7 Дефинирање на улогата и надлежностите на вооружените сили во заштита на воените КИИ и ВИИ и развој на соодветни капацитети.

4.1.8 Дефинирање и координација на военото планирање за начинот и употребата на воените сајбер капацитети со националната сајбер одбрана во разни ситуации.

Имплементација

Имплементацијата на Стратегијата ќе се реализира согласно Акцискиот план и ќе биде предмет на постојана годишна анализа иоценување, со конкретни предлози за унапредување. Земајќи во предвид дека современите технологии се во постојан развој и речиси е невозможно да се предвидат новите трендови на развој, неопходно е Стратегијата да биде подложена на постојано ажурирање согласно анализите и укажаните потреби.

Заклучок

Имплементацијата на стратешките цели и активностите дефинирани во стратегијата и акцискиот план мора да обезбедат воспоставување ефикасен систем за сајбер одбрана. Континуираното инвестирањето во градењето на способностите и капацитетите за ефективна сајбер одбрана ќе обезбеди квалитетни и технолошки развиени институции кои ќе можат ефикасно и ефективно да се справуваат со предизвиците во сајбер просторот.

АНЕКС

Акроними

Армија – Армија на Република Северна Македонија

ВИИ – Важни информацискисистеми

ЕУ – Европска Унија

КИИ - Критичната информациска инфраструктура

КИС – Комуникациско информациски системи

НАТО – Организација на северноатлански договор

ООН – Организација на Обединети Нации

CIRT – Тим за справување со компјутерски инциденти (Computer IncidentsResponse Team)

CCDCOE –НАТО Центар за кооперативна сајбер-одбрана (NATO Cooperative Cyber Defence Centre of Excellence)

Република Северна Македонија

Министерство за одбрана

Бр. 02-1249/2

12.02.2020 година

МИНИСТЕРКА ЗА ОДБРАНА

Радмила Шекеринска-Јанковска

СТРАТЕГИЈА ЗА САЈБЕР ОДБРАНА
АКЦИСКИ ПЛАН ЗА ИМПЛЕМЕНТАЦИЈА
2019 - 2023

Вовед

Целта на овој документ е да ги дефинира чекорите во имплементацијата на Стратегијата за сајбер одбрана на Република Северна Македонија. Во Министерството за одбрана на Република Северна Македонија и Армијата на Република Северна Македонија, се оформи работна група одговорна за развивање на стратешки документи од областа на сајбер одбраната. Работната група ги имаше во предвид веќе донесената Национална стратегија за сајбер безбедност, Стратешкиот одбранбен преглед, ДПРОС, Акцискиот план за членство во НАТО и Планот за интеграција во НАТО, како и НАТО политиката за сајбер одбрана и Акцискиот план за сајбер одбрана, врз база на што е изработена Стратегијата за сајбер одбрана.

Овој Акциски план ги вклучува главните активности потребни за зајакнување на капацитетите за сајбер одбрана, согласно предложената и усвоена Стратегија.

Број на активност	Активност	Код	Начин на имплементација (Задачи)	Носител	Соработници	рок
ЦЕЛ 1. СПОСОБНОСТИ ЗА САЈБЕР ОДБРАНА						
Ц1.1	Национални способности за сајбер одбрана	1.1.1	Развој на соодветни способности и ефикасни капацитети за сајбер одбрана кај сите конституенти што се дел од националната одбрана.	Министерство за одбрана на Република Северна Македонија/Армија	сите конституенти дел од националниот систем за сајбер одбрана	2019-2023
		1.1.2	Дефинирање на критериуми за евалуација на сајбер одбранбените капацитети и способности	Министерство за одбрана на Република Северна Македонија/Армија	сите конституенти дел од националниот систем за сајбер одбрана	6 месеци по донесување на национални критериуми за евалуација на КИИ
		1.1.3	Анализа, евиденција и евалуација на постоечката инфраструктура и институционалните капацитети со кои располага државата, јавниот и приватниот сектор, а кои можат да се искористат за потребите на сајбер одбраната.	Министерство за одбрана на Република Северна Македонија/Армија	сите конституенти дел од националниот систем за сајбер одбрана	2019-2023
		1.1.4	Изработка и имплементација на мерки за стратешко раководење со националните капацитети за сајбер одбраната согласно Законот за одбрана и други поврзани национални регулативи	Министерство за одбрана на Република Северна Македонија/Армија	сите конституенти дел од националниот систем за сајбер одбрана	1 година по 1.1.3
Ц1.2	Воени способности во Министерство за одбрана на Република Северна Македонија и Армијата за справување со закани во сајбер просторот	1.2.1	Формирање и развој на Воен тим за следење, координација и справување со компјутерски инциденти (MIL-CIRT).	Армија	Министерство за одбрана на Република Северна Македонија	2019 основна способност 2020-2023 финална способност
		1.2.2	Развој на способности и капацитети за сајбер одбрана во Министерство за одбрана на Република Северна Македонија и Армијата.	Министерство за одбрана на Република Северна Македонија/Армија		2019-2023
		1.2.3	Формирање и воспоставување на Воен авторитет за сајбер одбрана.	Армија	Министерство за одбрана на Република Северна Македонија	2020-2021
		1.2.4	Континуирано обезбедување на доверливост, интегритет и достапност на податоците и информациите за воените мрежи и системи.	Армија	Министерство за одбрана на Република Северна Македонија	2019/континуирано
		1.2.5	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 системите и мрежите на Министерство за одбрана на Република Северна Македонија и Армијата низ кои се процесираат класифицирани информации	Министерство за одбрана на Република Северна Македонија/Армија	сите конституенти дел од националниот систем за сајбер одбрана	2019-2020

Број на активност	Активност	Код	Начин на имплементација (Задачи)	Носител	Соработници	рок
		1.2.6	Развој на распоредливи капацитети за сајбер одбрана компатибилни со НАТО на рамниште на команда на ЛПБГ	Армија	Министерство за одбрана на Република Северна Македонија	2020-2024
		1.2.7	Идентификација на потребите за сајбер професионалци и дефинирање на базен на потенцијални човечки ресурси	Министерство за одбрана на Република Северна Македонија/Армија/Воена Академија		2020
		1.2.8	Развивање мотивирачки систем на награди и унапредувања на стручниот персонал од областа на сајбер безбедноста и одбраната, заснован на квалитетот и покажаните резултати на кадарот преку определување додаток на плата на стручниот персонал од областа на сајбер безбедноста и одбраната, во зависност од работните задачи, стручноста и незаменливоста	Министерство за одбрана на Република Северна Македонија/Армија		2020
		1.2.9	Формирање на активна резерва за потребите на сајбер одбраната и соодветно дефинирање на политики за регрутација и ангажман на стручни лица од оваа област	Армија	Министерство за одбрана на Република Северна Македонија	2020
		1.2.10	Воспоставување програми за размена на искуства со експерти од цивилни компании со цел подобрување на обученоста на кадарот за сајбер одбрана	Министерство за одбрана на Република Северна Македонија/Воена Академија	академска заедници/организации	2020-2022

Број на активност	Активност	Код	Начин на имплементација (Задачи)	Носител	Соработници	рок
ЦЕЛ 2: ЕДУКАЦИЈА И ОБУКА						
Ц.2.1	2.1. Континуирана едукација за обезбедување на високо ниво на свесност и лична одговорност во однос на сајбер одбраната во контекст на националната одбрана и безбедност	2.1.1	Подигнување на свеста за сајбер одбрана преку едукација и обука на целиот персонал во Министерство за одбрана на Република Северна Македонија и Армијата.	ВоенаАкадемија/ Министерство за одбрана на Република Северна Македонија/Армија		2019 /континирано согласно усвоениот план за обука 2018 година
		2.1.2	Дефинирање и континуирано едуцирање на потребен број на експерти за стратегиска, оперативна и тактичка сајбер одбрана и за менаџмент со сајбер заканите во Министерство за одбрана на Република Северна Македонија и Армијата.	ВоенаАкадемија/ Министерство за одбрана на Република Северна Македонија/Армија		2019 - континуирано согласно годишен план за школување и обука
		2.1.3	Формирање и воспоставување на Институт за Сајбер безбедност и дигитална форензика во рамките на Воената академија, со основна цел истражување, едукација и обука во делот на сајбер одбраната	ВоенаАкадемија		2020-2023
		2.1.4	Активно учество во НАТО кооперативниот центар за извонредност за сајбер одбрана (CCDCOE) со испраќање на национални експерти и учество во истражувачките активности на Центарот	ВоенаАкадемија/ Министерство за одбрана на Република Северна Македонија/Армија		2020/континуирано
		2.1.5	Креирање и развој на симулациски сценарија и програми за сајбер безбедносни инциденти што ќе се користат во националните вежби за сајбер одбрана	ВоенаАкадемија/ Министерство за одбрана на Република Северна Македонија/Армија		континуирано по потреба согласно 2.1.6
		2.1.6	Организација на национални вежби за сајбер одбрана во соработка со сите чинители што се дел од системот за националната одбрана.	Министерство за одбрана на Република Северна Македонија/Армија/Воена Академија	сите конституенти дел од националниот систем за сајбер одбрана	континуирано/минимум една вежба годишно
		2.1.7	Интеграција на сегментот на сајбер одбраната во сите оперативни вежби на национално ниво, во делот за национална одбрана.	Министерство за одбрана на Република Северна Македонија/Армија	сите конституенти дел од националниот систем за сајбер одбрана	2019/континуирано согласно планот за оперативни вежби
		2.1.8	Активно учество на меѓународни воени вежби и обуки за сајбер одбрана.	Министерство за одбрана на Република Северна Македонија/Армија		континуирано согласно годишен план за вежби и обуки

Број на активност	Активност	Код	Начин на имплементација (Задачи)	Носител	Соработници	рок
		2.1.9	Заедничкото споделување на капацитети и искуства со НАТО и партнерски држави.	Министерство за одбрана на Република Северна Македонија/Армија/Воена Академија		континуирано согласно билатерални, мултилатерални меморандуми за соработка и активности во годишните планови
ЦЕЛ 3: СОРАБОТКА И РАЗМЕНА НА ИНФОРМАЦИИ						
Ц.3.1	Воспоставување и одржување на взаемна меѓународна соработка и размена на податоци за одвраќање на споделените сајбер закани и зголемување на националната, регионалната и меѓународната безбедност и стабилност	3.1.1	Развој и имплементација на систем и програма 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.	Министерство за одбрана на Република Северна Македонија/Армија/Воена Академија	сите конституенти дел од националниот систем за сајбер одбрана	2020-2023
		3.1.2	Развој на цивилно-воена соработка за потребите на сајбер одбраната и промовирање на соработка помеѓу јавниот и приватниот сектор.	Министерство за одбрана на Република Северна Македонија/Армија/Воена Академија	сите конституенти дел од националниот систем за сајбер одбрана	2019-2020
		3.1.3	Воспоставување на соработка и размена на информации од доменот на сајбер одбрана помеѓу сите конституенти на системот за национална одбрана.	Министерство за одбрана на Република Северна Македонија/Армија/Воена Академија	сите конституенти дел од националниот систем за сајбер одбрана	2019-2022
		3.1.4	Дефинирање на национална точка за контакт со НАТО во поглед на сајбер операции и соработка	Министерство за одбрана на Република Северна Македонија/Армија	сите конституенти дел од националниот систем за сајбер одбрана	2020-2021
		3.1.5	Воспоставување на точка за безбедна комуникација со НАТО.	Министерство за одбрана на Република Северна Македонија/Армија	ДБКИ/МНР	2020
		3.1.6	Вклучување на Република Северна Македонија во колективната сајбер одбрана на НАТО и воспоставување на систем за соработка и размена на информации.	Министерство за одбрана на Република Северна Македонија/Армија	сите конституенти дел од националниот систем за сајбер одбрана	2020-2023
		3.1.7	Воспоставување и одржување на соработка со други партнерски држави во областа на сајбер одбраната	Министерство за одбрана на Република Северна Македонија/Армија/Воена Академија	партнерски држави	2019/континуирано
ЦЕЛ 4: ПРАВНА И РЕГУЛАТОРНА РАМКА						

Број на активност	Активност	Код	Начин на имплементација (Задачи)	Носител	Соработници	рок
Ц.4.1.	Креирање единствена и сеопфатна правна рамка за сајбер одбрана, земајќи ја предвид позитивната законска регулатива во Република Северна Македонија и директивите од НАТО и ЕУ	4.1.1	Развој и имплементација на систем и програма 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 ККИИ и ВКИИ	Министерство за одбрана на Република Северна Македонија	Армија/Воена Академија	2020-2021
		4.1.2	Развој на нови и усогласување на постоечките регулативиза сајбер безбедност и одбрана, согласно позитивната законска регулатива во Република Северна Македонија и директивите од НАТО и ЕУ.	Оперативно тело за сајбер безбедност	Министерство за одбрана на Република Северна Македонија/Армија/ Воена Академија	согласно активностите на Оперативното тело
		4.1.3	Дефинирање и имплементација на мерки за стратешко раководење со сајбер одбраната во Министерство за одбрана на Република Северна Македонија и Армијата	Министерство за одбрана на Република Северна Македонија	Армија	2019-2020
		4.1.4	Развој на методологија за процена на ризици од сајбер закани на ниво на Министерство за одбрана на Република Северна Македонија и Армијата.	Министерство за одбрана на Република Северна Македонија	Армија/Воена Академија	1 година по завршување на Cyber Risk Assessment на националната КИИ
		4.1.5	Развој на оперативни планови кај сите даватели на услуги во сајбер просторот согласно планот за одбрана.	Министерство за одбрана на Република Северна Македонија	сите конституенти дел од националниот систем за сајбер одбрана	2020 - согласно усвоен план за одбрана
		4.1.6	Развој на систем и процедури за размена на информации за заканите и ризиците во полето на сајбер одбраната на меѓународно ниво.	Министерство за одбрана на Република Северна Македонија	Армија	2020-2023
		4.1.7	Дефинирање на улогата и надлежностите на вооружените сили во заштита на воените КИИ и ВИИ и развој на соодветни капацитети.	Армија	Министерство за одбрана на Република Северна Македонија	2 години по 1.1.4
		4.1.8	Дефинирање и координација на военото планирање за начинот и употребата на воените сајбер капацитети со националната сајбер одбрана во разни ситуации.	Армија	Министерство за одбрана на Република Северна Македонија	2021