

**НАЦИОНАЛНА СТРАТЕГИЈА**  
**ЗА САЈБЕР БЕЗБЕДНОСТ**  
**НА РЕПУБЛИКА МАКЕДОНИЈА**  
**2018 - 2022**

## Содржина

<b>Резиме</b> .....	1
<b>Вовед</b> .....	4
<b>Сајбер трендови, предизвици и закани</b> .....	7
<b>Принципи на сајбер безбедноста</b> .....	13
Ефективни и ефикасни капацитети за сајбер безбедност .....	13
Заштита и превенција .....	13
Сигурност за економски развој .....	14
Доверба и достапност .....	14
Правна сигурност .....	15
<b>Засегнати страни</b> .....	16
<b>Визија и мисија</b> .....	18
<b>Цели</b> .....	19
<b>ЦЕЛ 1: Сајбер отпорност</b> .....	20
<b>ЦЕЛ 2: Сајбер капацитети и култура за сајбер безбедност</b> .....	22
<b>ЦЕЛ 3: Справување со сајбер криминал</b> .....	25
<b>ЦЕЛ 4: Сајбер одбрана</b> .....	27
<b>ЦЕЛ 5: Соработка и размена на информации</b> .....	29
<b>Имплементација</b> .....	32
<b>Национален совет за сајбер безбедност</b> .....	32
<b>Тело со оперативни капацитети за сајбер безбедност</b> .....	33
<b>Предизвици за имплементација</b> .....	35
<b>АНЕКС 1</b> .....	37
<b>Дефиниции</b> .....	37
<b>АНЕКС 2</b> .....	42
<b>Акроними</b> .....	42

Верзионирање:

Верзија	Дата	Забелешки
1.0	11.06.2018	Работна верзија
1.1	03.07.2018	Нацрт верзија со имплементирани коментари од засегнати страни
1.2	17.07.2018	Финална верзија, усвоена од Владата на Република Македонија

## Резиме

Зајакнувањето на националните капацитети за справување со сајбер закани и подобрувањето на сајбер безбедноста на национално ниво се од приоритетно значење за Република Македонија.

Националната стратегија за сајбер безбедност на Република Македонија е стратешки документ кој треба да служи како патоказ за развој на сигурно, безбедно, доверливо и отпорно дигитално окружување, поддржано од квалитетни капацитети, кои се базираат на доверба и соработка во полето на сајбер безбедноста. Овој документ е организиран во седум дела.

**Првиот дел** од оваа стратегија е вовед во проблематиката со посебен акцент кон зголемената зависност од услугите во сајбер просторот, зголемена употреба на информациските и комуникациските технологии (ИКТ) и негативното влијание од комплексни сајбер напади врз функционирањето на јавниот и приватниот сектор. Овој дел се фокусира на потребата од постоење на стратешки документи поврзани со зајакнувањето на националните капацитети за сајбер безбедност.

Предмет на анализа во **вториот дел** од оваа стратегија се глобалните и локалните сајбер трендови, предизвици и закани кои се клучни во однос на функционирањето на сајбер просторот на Република Македонија.

**Третиот дел** ги вбројува принципите кои ја поддржуваат Стратегијата:

- Ефективни и ефикасни капацитети за сајбер безбедност,
- Заштита и превенција,
- Сигурност за економски развој,
- Доверба и достапност и
- Правна сигурност.

Во **четвртиот дел** се дефинирани сите засегнати страни во полето на сајбер безбедност кои се вклучени во Стратегијата: јавен сектор, приватен сектор, академска заедница, граѓани и граѓански здруженија.

**Петтиот дел** ги опфаќа визијата и мисијата на Националната стратегија за сајбер безбедност на Република Македонија.

Во **шестиот дел**, поставени се 5С - цели на Националната стратегија за сајбер безбедност. Овие цели се дефинирани во насока на:

1. Воспоставување на ИКТ инфраструктура отпорна на сајбер закани, идентификување и имплементирање на соодветни решенија за заштита на националните интереси.
2. Промовирање на култура за сајбер безбедност, со цел сеопфатно разбирање на сајбер заканите, како и градење и унапредување на потребните капацитети за заштита.
3. Зајакнување на националните капацитети за превенција, истражување и соодветен одговор на сајбер криминалот.
4. Зајакнување на капацитетите за одбрана на националните интереси и намалување на тековните и идните ризици во сајбер просторот.
5. Соработка и размена на информации на национално и меѓународно ниво.

**Седмиот дел** е посветен на генерализација на Акцискиот план за имплементација на Националната стратегија за сајбер безбедност, како и на претставување на дел од предизвиците за успешна имплементација. Во овој дел се дефинирани одговорностите кои се однесуваат на органите на власта, во насока на поддршка на целите и активностите дефинирани во стратегијата. Исто така, поставена е организациската структура за координација и имплементација на активностите дефинирани во стратегијата и акцискиот план. Во оваа насока, успешната реализација на оваа стратегија подразбира оформување на Национален совет за сајбер безбедност и Тело со оперативни капацитети за сајбер безбедност чиешто надлежности и активности се дефинирани подолу.

Акцискиот план, кој ќе ги содржи мерките и активностите за реализирање на поставените цели, ќе биде изготвен во рок од три месеци од усвојување на оваа Стратегија од страна на Владата на Република Македонија.

Националната Стратегија за сајбер безбедност е базирана на принципите на ЕУ (Cybersecurity Strategy of the European Union) и НАТО (NATO Cyber Defence Pledge) и други меѓународни организации.

## Вовед

Во последните години, употребата на информациско-комуникациските технологии (ИКТ) во континуитет се зголемува. Воедно, оваа експанзија е основен двигател на глобализацијата и дава значителен придонес во развојот на економијата, животниот стандард и благосостојбата на целото општество.

Брзиот напредок на ИКТ дава значителни придобивки за напредно функционирање и развој на македонското општество. Сите чинители од политичкиот, општествениот и економскиот живот во Република Македонија ги користат можностите што ги нуди огромната експанзија на ИКТ. Според глобалните индекси за развој на информатичкото општество (IDI, NRI, EGDI, GCI), нивото на развој на Република Македонија во областа на информатичкото општество се наоѓа во првата статистичка третина. Министерството за информатичко општество и администрација и други надлежни институции во континуитет воведуваат нови електронски услуги со цел да го олеснат секојдневното функционирање на граѓаните.

Сепак, зголемената зависност од услугите обезбедени во сајбер просторот значи дека нефункционалните ИКТ системи и сериозните сајбер напади можат да имаат значително негативно влијание врз функционирањето на јавниот и приватниот сектор, како и на целото општеството. Зависноста од новите технологии и потребата од поголема достапност на услугите во сајбер просторот е причина корисниците и институциите да ја зголемат свесноста за значењето на интегритетот, автентичноста и доверливоста на податоците. Македонските комуникациски мрежи се дел од глобалните комуникациски мрежи, што подразбира дека сајбер безбедносните инциденти на друго место можат да влијаат врз македонскиот сајбер простор и услуги, и обратно.

Земајќи ги предвид анализите направени од најрелевантните светски институции во доменот на безбедноста и одбраната, несомнено е дека во последните години сајбер заканите се меѓу најзначајните безбедносни закани врз современите

општества, што е основна причина истите да се третираат како интегрален дел од националната и меѓународната безбедност.

Од претходно наведените причини, зајакнувањето на националните капацитети за справување со сајбер заканите и зголемувањето на сајбер безбедноста станаа еден од клучните предизвици на Република Македонија.

Постоењето на стратешки документи поврзани со овој предизвик е од клучно значење во напорите за зајакнување на капацитетите во областа на сајбер безбедноста. Развојот на Национална стратегија за сајбер безбедност има основна функција да ги подобри рамковните услови во оваа област. Потребата од развој и донесување на Национална стратегија за сајбер безбедност главно е поврзана со следното:

1. Активностите, социјалните интеракции, економијата, како и основните човекови права и слободи се тесно поврзани со примената на ИКТ, поради што е неопходно да се обезбеди отворен, сигурен и безбеден сајбер простор;
2. Употребата на ИКТ системите и развојот на електронските услуги го зголемува ризикот од сајбер инциденти и злоупотреби, што ги прави овие закани едни од посериозните врз националната безбедност;
3. Дефинирање и развој на политика за сајбер одбрана;
4. Воспоставување интегриран, мултидисциплинарен пристап за обезбедување поблиска соработка и координација меѓу одбранбениот и безбедносниот сектор, институции вклучени во борбата против сајбер криминалот, приватниот сектор, граѓаните и граѓанските организации, како и други релевантни засегнати страни;
5. Зајакнување на оперативниот капацитет, координација и соработка помеѓу релевантните институции и организации вклучени во борбата против сајбер криминалот;
6. Воспоставување заеднички стандарди, обука и едукација на сите институции и организации вклучени во развојот на сајбер безбедноста;



7. Зајакнување на институционалната и законската рамка во областа на сајбер безбедноста.
8. Зајакнување на националните капацитети за превенција и заштита од сајбер напади, како и спроведување активности за подигнување на националната свест за сајбер безбедност.

Националната стратегија за сајбер безбедност е развиена во согласност со 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 во корист на граѓаните, бизнисите и јавната администрација.

## Сајбер трендови, предизвици и закани

### Зголемен број Интернет и ИКТ корисници и зголемена зависност од ИКТ системи

Зголемениот број Интернет корисници (во првиот квартал од 2017, 73.6% од домаќинствата имале пристап до Интернет во домот) и ИКТ корисници, заедно со порастот на употребата на Интернетот во бизнис секторот (почнувајќи од јануари 2017, 91.2% од бизнис претпријатијата со 10 или повеќе вработени имале широкопојасна Интернет конекција) предизвикува сè поголема зависност од глобалната поврзаност. Прекин во нудењето на одредени услуги кои се зависни од ИКТ, што може да предизвика и каскаден ефект, може да биде од критично значење за функционирањето на државата, особено кога се работи за критичната информациска инфраструктура (во понатамошниот текст "КИИ") и други важни информациски системи (во понатамошниот текст "ВИС").

### Имплементацијата на електронски услуги

Имплементацијата на електронските услуги во Република Македонија значително ќе ги подобри процесите и функционирањето на општеството. Сепак, треба да се земе предвид дека електронските услуги и апликации ќе донесат и нови предизвици и сајбер ризици.

### Ниско ниво на сајбер безбедност во малите и средните претпријатија

Сè поголема е потребата од подигнување на свеста за примена на најдобри практики за заштита на ИКТ и информациите во малите и средните претпријатија. Истите често не се во состојба да ги дефинираат нивните потреби за сајбер безбедност, а исто така во голем број случаи немаат ниту доволно ресурси и знаења кои се неопходни за надминување на евидентираниите проблеми во оваа област. Од друга страна, во одредени случаи, податоците и системите на овие претпријатија можат да бидат од критично значење за државата, посебно доколку истите се ангажирани како подизведувачи во поголеми претпријатија и институции.

## Зголемена зависност на одбранбениот и безбедносниот сектор од ИКТ

Одбранбениот и безбедносниот сектор сè повеќе се зависни и се темелат на функционалноста на ИКТ системите. Ранливоста на овие технологии и опасноста од нивно нарушување или уништување ги зголемува ризиците од негативно влијание врз основните одбранбени и безбедносни способности и исполнувањето на критериумите за полноправно членство во ЕУ и НАТО .

### Сајбер криминал

Глобалната поврзаност, која доколку се користи на соодветен начин може да обезбеди и целосна анонимност, ги зголемува можностите на злонамерните корисници за пристап, кражба и злоупотреба на чувствителни информации. Голем дел од злонамерните корисници и криминални организации го препознаа сајбер просторот како можност за брза добивка, притоа овозможувајќи им намален ризик од нивно откривање. Глобализацијата и анонимноста им овозможуваат на злонамерните корисници полесни напади кон претходно точно дефинирани жртви, но воедно и реализирање на многу поголеми операции и напади од многу поголеми размери.

### Закани и ризици поврзани со употребата на социјалните мрежи

Сè поголемиот број на социјални мрежи, зголемениот број на корисници на овие мрежи, како и напредокот на алгоритмите за препознавање лица, е основа за зголемен ризик од загуба на приватноста, крадење на лични податоци, како и крадење на дигиталниот идентитет. Цел на овие напади можат да бидат физички или правни лица.

### Ниско ниво на свесност за заканите во сајбер просторот кај крајните корисници

Голем дел од Интернет корисниците во јавниот и приватниот сектор, како и сите останати корисници, немаат или имаат ниско ниво на познавања за најчестите сајбер напади (како што се фишинг, лажни е-продавници итн.), што е причина голем

дел од нив да бидат жртви на напад за кој постојат едноставни превентивни и одбранбени механизми.

## Зголемена потреба од експерти за сајбер безбедност

Постоечките наставни програми на сите нивоа на образование (основно и средно образование, како и сите циклуси на студии на универзитетите во Република Македонија) не ги задоволуваат во целост потребите за едуцирање и обука на стручни лица кои ќе одговорат на најновите предизвици и трендови во сајбер просторот. Од друга страна, потребата од вакви експерти е сè поголема.

## Несоодветна сајбер хигиена

Една од причините за широко распространети успешни сајбер напади е непочитувањето на таканаречената „сајбер хигиена“ од страна на корисниците и организациите. Главен предизвик е тоа што организациите сметаат дека е многу тешко да се воспостави активна контрола над сајбер хигиената на нивните вработени и на тој начин ефективно да ги санираат сајбер безбедносните ризици. Исто така, еден од предизвиците е зголемената комплексност за одржување на основна сајбер хигиена, како што се идентификување на нивните средства, ажурирање на софтвер, инсталирање закрпи, управување со стандарди, едукација и обука на корисниците во поголемите организации. Земајќи предвид дека најголем дел од сите сајбер закани се превенираат со решавање на прашањето за сајбер хигиена, ова прашање е едно од клучните од аспект на сајбер безбедноста.

## Интернет на нештата

Додека бројот на уреди поврзани на Интернет значително се зголемени, повеќето корисници ја игнорираат потребната сајбер хигиена, односно како да се однесуваат и како да ги заштитат уредите што ги користат. Концептот "Интернет на нештата" го засилува овој предизвик. Традиционалните електронски уреди, како што се персоналните и преносните компјутери, автоматски го активираат антивирусниот софтвер, firewall-ите итн., но истото не е случај со други паметни уреди како телевизори, фрижидери, видеонадзор итн.. Од таа причина, во последниот период

забележана е драстично зголемен број на онлајн злоупотреба на овие уреди, а во иднина заканите врз и од овие уреди ќе бидат во значително поголема мера.

## Вештачката интелигенција

Полето на вештачката интелигенција, поточно машинското учење, веќе има значајна улога во денешното глобално општество. Континуираниот развој во овие полиња има позитивно влијание и веќе се применува за усовршување на безбедносните механизми за заштита од разни сајбер закани. Од друга страна, вештачката интелигенција станува и еден од главните предизвици во областа на сајбер безбедноста и заштитата на приватноста, затоа што истата технологија се искористува и кај злонамерниот софтвер.

## Зголемување на бројот и софистицираноста на злонамерниот софтвер

Во последниот период се соочуваме со сè поголем број и сè пософистицирани злонамерни софтвери. Стотици илјади нови злонамерни софтвери секојдневно се продуцираат, а воедно злонамерните корисници преку различни механизми значително ги ограничуваат опциите за следење на изворот на нападот, односно обратното инженерство и форензичка анализа. Дополнително, во последните години еден од најголемите трендови е зголемениот број на регистрирани злонамерни софтвери кои ги напаѓаат мобилните уреди. Причина за ова е што во основа мобилните апликации се поранливи, а и тоа што голем дел од корисниците не преземаат основни безбедносни мерки за заштита на нивните мобилни уреди (како на пример инсталирање на антивирусен софтвер).

## Компромитиран хардвер и софтвер

Зголемениот број на корисници и добавувачи на ИКТ го зголемува ризикот од т.н. напади во синџирот на снабдување, каде што комерцијалните хардверски и софтверски компоненти кои се продаваат како готови производи, се компромитирани со безбедносни слабости, злонамерен код или вградени "задни врати". Недоволната валидација на комерцијалните хардверски и софтверски компоненти може да доведе до кражба на чувствителни и лични податоци, сајбер

шпионажа или ненамерно учество во злонамерни активности (на пример, напади базирани на ботнети).

## Голема количина на податоци (Big data) и услуги во облак

Заштитата и безбедноста на податоците, особено на оние од јавен интерес (податоци релевантни за КИИ и ВИС) се клучни за Република Македонија. Количината на податоци кои се обработуваат и во јавниот и во приватниот сектор секојдневно се зголемува, а со тоа се зголемува и потребата за нивно складирање. Така се појавија нови форми на складирање на податоци, како што се складирање во облак. Сепак, употребата на онлајн услуги и облаци може да доведе до употреба на несоодветни безбедносни решенија со сомнителен кредибилитет.

## Сајбер-физички закани врз индустриските контролни системи и критичната инфраструктура

Следејќи ги глобалните трендови, постои реална можност во наредниот период јавниот и приватниот сектор да се соочат со зголемен број сајбер напади, вклучувајќи и индустриска сајбер шпионажа, сајбер вандализам и идентификација на ранливости кај енергетскиот сектор, финансискиот сектор, здравствениот сектор, транспортните системи и други делови од КИИ и ВИС. Притоа, може да се очекува различен пристап, од предизвикување на непосредни прекин во функционирањето на делови од критичната инфраструктура до целосно блокирање. Нефункционалноста на гореспоменатите системи може да има фатални последици, а поради висока хетерогеност на техничките решенија, подоцнежната техничка анализа е значително отежната.

## Ботнети и DDoS/DoS напади

„Ботнетите“ се најчесто искористени за реализирање на DDoS/DoS напади, и се сè поробусни, отпорни и тешки за откривање и следење. Развојот во областа на „интернет на нештата“, кои најчесто имаат слаби безбедносни механизми, значително ја зголемуваат опсегот и капацитетите за напад кои би ги имале на располагање злонамерните корисници.

## Ransomware

Бројот на нови ransomware злонамерни активности експоненцијално се зголемува, напаѓајќи ги сите сфери на општеството, вклучувајќи ја и КИС и ВИС. Овој злонамерен софтвер, иако е едноставен по природа, може да предизвика голема штета преку криптирање на датотеки или оневозможување пристап кон одредена апликација или оперативниот систем. Со цел да добијат пристап кон сопствените податоци, т.е. да бидат во можност да ги декриптираат податоците, голем дел од жртвите се подготвени да платат одредена сума на напаѓачите кои го развиле и дистрибуирале злонамерниот софтвер. Најчесто овие активности се преземаат од криминални организации кои имаат единствена цел финансиска добивка, но во одредени случаи имаат основна задача да оштетат одредени ИКТ системи и податоци, без притоа да постои можност за враќање на податоците (NotPetya). Иако ransomware најчесто е насочен кон поединци, сè поголем е бројот на случаи каде како жртви се јавуваат и претпријатија и институции.

## Рударење криптовалути

Злоупотребите поврзани со криптовалути се директна кражба на истите од нивните сопственици, но и кражба на компјутерски ресурси со цел злонамерните корисници да се здобијат со поголем капацитет за рударење на криптовалути. Нападот не е насочен само кон обичните корисници, туку и кон помоќни компјутерски системи кои често се од витално значење, што може да предизвика значителна штета.

## Сајбер шпионажа

Зголемениот процент на дигитализација на општеството и индустријата доведува до појава на нови начини преку кои одредени ентитети или поединци можат да добијат неовластен пристап до осетливи или доверливи информации. Со вакви активности можат да бидат нанесени големи штети на државните интереси, бизнис плановите и угледот на компаниите, како и граѓаните.

## Принципи на сајбер безбедноста

### Ефективни и ефикасни капацитети за сајбер безбедност

Огромниот технолошки развој и сè поголемата примена на новите достигнувања во ИКТ им овозможува на злонамерните корисници да наоѓаат нови механизми за нарушување на сајбер безбедноста, поради што е повеќе од неопходно информациско-комуникациската инфраструктура во Република Македонија да биде подготвена да одговори на предизвиците во сајбер просторот.

Со цел да се одговори на најновите ризици и закани, Република Македонија ќе ги поддржи истражувањето и развојот во областа на сајбер безбедноста, како и образованието и обуката на сите нивоа во општеството, вклучувајќи ја и обуката на крајните корисници.

Ефективен производ од истражување и развој во областа на сајбер безбедноста може да се постигне само со тесна соработка помеѓу сите засегнати страни. Затоа, Република Македонија во целост го поддржува мулти-секторскиот пристап за градење на ефикасни капацитети за сајбер безбедност.

Со цел ефективно справување и навремен одговор на современите сајбер закани, Република Македонија во целост ќе го поддржи зајакнувањето на постоечките капацитети и процедурите за соработка помеѓу сите релевантни ентитети или индивидуи во областа на сајбер безбедноста.

### Заштита и превенција

Сериозните сајбер закани врз безбедноста на Република Македонија, меѓу кои сајбер операциите и шпионажата спонзорирани од други држави (вклучувајќи кражба на интелектуална сопственост од критични државни институции, КИИ и ВИС), употребата на сајбер просторот за поддршка на терористички активности, се третираат како ризици врз националната безбедност. Еден од главните принципи на ова Стратегија е поддршка на системот за обезбедување на национална безбедност на Република Македонија.



## Сигурност за економски развој

Развојот на безбедно општество и примената на сите безбедносни практики и процеси преку соработка на сите засегнати страни ќе обезбеди бизнисите да останат доверливи и достапни за клиентите, а со самото тоа и профитабилни. Зголемување на довербата на граѓаните во дигиталните сервиси и електронската трговија директно ќе придонесе во развојот на дигиталната економија. Ова ќе придонесе Република Македонија да биде препознаена како сигурно место за инвестирање и деловно работење.

Имплементацијата на најнови ИКТ решенија и практики и глобалната поврзаност ќе го поддржи економскиот раст, а воедно ќе се минимизираат негативната екстерналија како последица од безбедносни инциденти во сајбер просторот.

## Доверба и достапност

Одговорот на предизвиците во сајбер просторот може да биде успешен само во случај на добро изградени процедури за соработка помеѓу сите засегнати страни кои можат да дадат свој придонес во делот на сајбер безбедноста. Поради оваа причина, потребна е тесна соработка помеѓу јавниот сектор, приватниот сектор и граѓанскиот сектор.

Заштитата на КИИ и ВИС е од клучно значење за Република Македонија. Земајќи предвид дека најголем дел од оваа инфраструктура и услуги се во сопственост на приватниот сектор, нивната вклученост во процесите поврзани со заштита на сајбер безбедноста е клучна.

И покрај сите превентивни мерки за безбедност и заштита, појавата на инциденти е неизбежна, што претставува ризик по достапноста на КИИ. Координираните активности во плановите за обновување по појава на инциденти кај КИИ треба да бидат регулирани, а нивната ефективност редовно да се тестира преку заеднички сајбер вежби.

Со цел подобрување на соработката во областа на сајбер безбедноста помеѓу сите засегнати страни, Република Македонија ќе формира Центар за извонредност. Овој

Центар би имал за цел размена на искуствата помеѓу јавниот сектор, приватниот сектор (пред сè, компаниите кои управуваат со КИИ и ВИС), граѓанските организации, академијата и други организации.

## Правна сигурност

При имплементација на мерките во сајбер безбедноста потребно е да се почитуваат позитивните правни акти и неповредливоста на основните човекови права, демократски принципи и темелни вредности. Една од главните карактеристики на Интернетот е неговата отвореност и достапност за сите, во секое време и со загарантиран слободен проток на информации. Корисниците на услуги во сајбер просторот бараат истиот да биде доверлив и да им обезбеди интегритет на информациите, слобода на изразување, заштита на личните податоци и заштита на приватноста. Очекувањата на корисниците се да имаат слободен пристап кон интернет без било какво попречување, штета или незаконско следење на комуникацијата. Македонското законодавство, европската регулатива, како и позитивните меѓународни правни акти поврзани со човековите права, слободата на изразување и заштитата на приватноста се универзални и истите се применливи и во сајбер просторот.

## Засегнати страни

Дефинирањето на засегнатите страни во областа на сајбер безбедноста е важен сегмент кој ни овозможува понатамошно дефинирање на опфатот на Стратегијата.

Стратегијата ги опфаќа следните сектори:

1. **Јавен сектор**, во смисла на оваа Стратегија, се надлежни органи и други субјекти, кои на различни начини ги претставуваат корисниците на сајбер просторот и субјектите кои се обврзани да ги применуваат мерките кои произлегуваат од Стратегијата;
2. **Приватен сектор**, што е во тесна соработка со надлежните државни и регулаторни тела кои се засегнати страни на Стратегијата, особено правните лица кои се предмет на посебни прописи за критичната инфраструктура и системот за одбрана и безбедност, како и сите други правни и деловни субјекти кои на различни начини ги претставуваат корисниците на сајбер просторот и субјектите кои се обврзани да ги применуваат мерките кои произлегуваат од Стратегијата, со сите особености на тие правни и деловни субјекти, во поглед на нивниот обем на работа, бројот на вработените и пазарите кои ги покриваат;
3. **Академска заедница**, образовни институции од јавниот и од приватниот сектор кои на различни начини ги претставуваат корисниците на сајбер просторот и субјектите кои се должни да ги применуваат мерките што произлегуваат од Стратегијата. Воедно, академската заедница има улога во градење на соодветни кадри преку развој и имплементација на програми и обуки, како и нудење на експертиза во областа на сајбер безбедноста;
4. **Граѓани и граѓански организации**, каде се опфатени корисниците на ИКТ и услугите. Состојбата на безбедноста во сајбер просторот се одразува на граѓаните на различни начини. Таа, исто така, се однесува на граѓаните кои

не го користат активно сајбер просторот, но сепак таму можат да се најдат нивни лични податоци.

## Визија и мисија

### **Визија**

Република Македонија да има сигурно, безбедно, доверливо и отпорно дигитално опкружување, поддржано од квалитетно изградени капацитети, високо квалификувани експерти, изградено ниво на доверба и национална и меѓународна соработка во областа на сајбер безбедноста.

### **Мисија**

Република Македонија да има јасно дефинирани и одржливи политики, кои координирано ќе ги спроведува во насока на унапредување на националната сајбер безбедност.

## Цели

Петте цели 5C на Стратегијата за сајбер безбедност се состојат од пет клучни области и се наменети за зголемување на капацитетите за одбрана од сајбер закани и зголемување на безбедноста во сајбер просторот во сите сектори и на сите нивоа.

### Цел 5: Соработка и размена на информации

Република Македонија да го штити својот сајбер простор преку соработка и размена на информации на национално и меѓународно ниво, со цел да обезбеди отворен, слободен, доверлив и безбеден сајбер простор.

### Цел 1: Сајбер отпорност

Информациско-комуникациската инфраструктура во Република Македонија да биде отпорна на сајбер закани и да бидат идентификувани и имплементирани соодветни решенија за заштита на националните интереси.

### Цел 2: Сајбер капацитети и култура за сајбер безбедност

Јавниот, приватниот сектор и македонското општество да ги разбираат сајбер заканиите и да имаат капацитети да се заштитат.

### Цел 4: Сајбер одбрана

Република Македонија да ги зајакне своите капацитети за одбрана на националните интереси и да ги намали моменталните и идните ризиците во сајбер просторот.

### Цел 3: Справување со сајбер криминал

Република Македонија да ги зајакнува своите капацитети за превенција, истражување и соодветен одговор на сајбер криминал.



Слика 1: 5C цели на Стратегијата за сајбер безбедност

## ЦЕЛ 1: Сајбер отпорност

*Информациско-комуникациската инфраструктура во Република Македонија да биде отпорна на сајбер закани и да бидат идентификувани и имплементирани соодветни решенија за заштита на националните интереси.*

Сајбер отпорноста обезбедува доверливост, интегритет и достапност преку идентификација, заштита и воспоставување на претходна состојба од сајбер инциденти. Јавниот и приватниот сектор мора да имаат навремени и точни информации и предлози за подобрување на сајбер безбедноста и да бидат во можност меѓусебно да соработуваат во случај на сајбер инциденти. Потребно е да се идентификуваат сите релевантни капацитети за сајбер безбедност кај сите засегнати страни и преку дефинирање на конкретни надлежности и активности да се стават во функција на подобрување на сајбер безбедноста и во функција на справување со сајбер инциденти. Целта е да се обезбеди заштита на најважниот дел од инфраструктурата во Република Македонија, користење на соодветни решенија за одбрана на државните интереси од страна на надлежните институции и подготвеност за сериозни (комплексни) сајбер инциденти.

### **Активности:**

1. Унапредување на капацитетите и способностите на Националниот центар за одговор на компјутерски инциденти МКД-ЦИРТ.
2. Идентификација и заштита на КИИ и ВИС.
3. Користење на најдобри решенија за одговор на сајбер инциденти со цел заштита на националните безбедносни интереси.
4. Преземање мерки и активности за справување со сајбер инциденти од поголеми размери.
5. Развој на национални процедури во мирновремена, кризна, вонредна и воена состојба за управување со сајбер инциденти кои ќе овозможат ефикасна меѓу-институционална соработка, ќе ја дефинираат улогата на секоја институција, ќе ги дефинираат соодветните протоколи и процедури, како и начинот на комуникација, координација и размена на информации.

6. Развој на методологија за процена на ризици од сајбер закани на национално ниво.
7. Креирање единствена и сеопфатна правна рамка за сајбер отпорност, земајќи ја предвид позитивната законска регулатива во РМ и ЕУ.
8. Континуирано следење, прифаќање и имплементација на меѓународно признати стандарди и процедури во областа на сајбер безбедноста.
9. Континуирана надградба на националните стратешки документи земајќи ги предвид најновите стандарди и технологии за сајбер безбедност и сајбер закани.
10. 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.
11. Континуирано подобрување на отпорноста, интегритетот и доверливоста на КИИ и ВИС.
12. Континуирана анализа и мониторинг на сајбер законите и ризиците во Република Македонија преку редовно обезбедување информации од засегнатите страни.
13. 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.
14. Спроведување на редовни ревизии со цел детектирање на грешки и ранливости на информациските системи и мрежи кои се дел од КИИ и ВИС.
15. Континуирано унапредување на технолошките и организациските потреби за ефикасно справување со сајбер законите.
16. Зголемување на националните капацитети за активна сајбер одбрана и преземање на соодветни контрамерки за справување и одговор на сајбер закани.



## ЦЕЛ 2: Сајбер капацитети и култура за сајбер безбедност

*Јавниот, приватниот сектор и македонското општество да ги разбираат сајбер закани и да имаат капацитети да се заштитат.*

Оваа цел е повеќе од промовирање на свесноста за сајбер закани и се фокусира на градење капацитети за сајбер безбедност помеѓу засегнатите страни со активности во оваа област. Промовирањето на култура за сајбер безбедност значи поттикнување на одговорност и разбирање за сајбер ризиците во сите сфери на општеството, преку развивање на информирана доверба на корисниците во електронските сервиси, како и подобрување на знаењето како тие притоа да ги заштитат нивните лични податоци. Постигнувањето на оваа цел значи креирање вештини, знаења и решенија за заштита, притоа обезбедувајќи поголема отпорност од злонамерни сајбер активности.

Дополнително, оваа цел ќе овозможи ефикасна дисеминација на мерките и активностите за сајбер безбедност на сите нивоа, вклучувајќи ги засегнатите страни, за да се постигне потребното ниво на знаење и вештини на нивните вработени, корисници и останати трети страни инволвирани во процесите. Размената на вештини, знаења и искуства во областа на сајбер безбедноста на национално ниво ќе биде постигната преку креирање на ад-хок меѓу-ресорски истражувачки тимови составени од експерти од јавниот сектор, приватниот сектор и академската заедница.

Во контекст на обезбедување на соодветни сајбер капацитети бизнисите и организациите да можат да се справат со најсофистицирани и комплексни напади во сајбер просторот, ќе се обезбеди соодветно зголемување на експертизата во оваа област преку инвестирањето во сајбер безбедноста, што е основа за постигнување на конкурентни комерцијални перформанси.

### **Активности:**

1. Зголемување на капацитетите за сајбер безбедност во малите и средните компании.

2. Унапредување на капацитетите за сајбер безбедност во приватниот сектор, вклучувајќи ја и националната инфраструктура, КИИ и јавниот сектор.
3. Развој и промовирање на наставни програми и обуки во областа на сајбер безбедноста на сите нивоа.
4. Поддршка на истражувачки капацитети и бизнис иновации преку креирање на научно истражувачки центар во областа на сајбер безбедноста.
5. Учество во национални и меѓународни истражувачки проекти и активности поврзани со сајбер безбедноста.
6. Обезбедување едукација и обука и зголемување на свеста за сајбер безбедноста во приватниот сектор.
7. Обезбедување насоки за реакција во случај на сајбер инциденти, сајбер криза на сите нивоа на општеството, вклучувајќи и насоки за однесување во секојдневните активности.
8. Спроведување истражување и утврдување на националните приоритети и врз основа на тоа преземање активности и инвестиции за развој на сајбер безбедноста.
9. Обезбедување и примена на најсоодветни хардверски и софтверски решенија за превенција, идентификација и управување со сајбер инциденти.
10. Зголемување на свеста и основните познавања во областа на сајбер безбедноста на учениците во основните и средните училишта,
11. Усовршување на постоечките наставни програми во основните и средните училишта и вклучување на елементи од областа на сајбер безбедноста во новите универзитетски студиски програми со цел продуцирање на поквалитетни кадри од областа на сајбер безбедноста.
12. Зголемување на свеста и основните познавања во областа на сајбер безбедноста кај граѓани и граѓанските организации.
13. Обезбедување на соодветна едукација и обука во областа на сајбер безбедноста за персоналот во јавната администрација.

14. Обезбедување на соодветна едукација и обука во областа на сајбер безбедноста за менаџерски и раководен персонал во јавниот и приватниот сектор.
15. Обезбедување стручно-специјалистичко образование и обука за лицата кои работат во областа на сајбер безбедноста.
16. Воспоставување механизми за задржување на стручниот кадар од областа на ИКТ и сајбер безбедност.

### ЦЕЛ 3: Справување со сајбер криминал

*Република Македонија да ги зајакнува своите капацитети за превенција, истражување и соодветен одговор на сајбер криминал.*

Развојот и користењето на информациско-комуникациската технологија и системите за автоматско управување доведува до појава на различни видови на злоупотреби кои се карактеризираат како сајбер криминал. Сајбер криминалот се движи од злоупотреби и измами на Интернет до пософистицирани и покомплексни напади на информациските системи. Сајбер криминалот, исто така, може да биде мотивиран и извршен од различни причини и од различни сторители. Со оглед на широкиот спектар на сајбер криминалот и опфатот на релевантни национални институции и организации одговорни за справување со сајбер криминал, за оваа посебна цел неопходно е да се изготви детален план за справување со сајбер криминал на национално ниво, кој ќе го опфати и криминалот овозможен од сајбер просторот. Овој план треба да го дефинира проблемот со сајбер криминалот и предизвиците што ги генерира. Во истиот е потребно да бидат наведени активностите за превенирање од сајбер криминал и да се овозможи побезбедно функционирање на општеството. Една од поефикасните методи за превенција е преку нудење соодветни насоки и решенија за воспоставување или унапредување на хигиена за сајбер безбедност во општеството согласно најдобрите меѓународни практики. Меѓу-институционалниот и мулти-дисциплинарниот пристап со вклучување на сите засегнати страни е од клучно значење за да се обезбеди ефикасен одговор на сајбер криминалот.

#### **Активности:**

1. Унапредување на капацитетите за справување со сајбер криминал.
2. Хармонизација на националните со меѓународните политики поврзани со сајбер криминалот.
3. Креирање единствена и сеопфатна правна рамка за сајбер криминал, земајќи ја предвид позитивната законска регулатива во РМ и ЕУ.

4. Модернизација на надлежните институции за ефикасна борба против сајбер криминал.
5. Воспоставување ефикасни процедури за пријавување и истражување на сајбер криминал.
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.
7. Унапредување на соработката со регионалните и меѓународните организации за борба против сајбер криминалот.
8. Унапредување на постоечките и воспоставување на нови механизми за соработка и размена на информации со приватниот и граѓанскиот сектор.
9. Обезбедување стручно-специјалистичко образование и обука за лицата кои работат во областа на идентификација и истражување на сајбер криминал.
10. Креирање мултидисциплинарна академска средина за унапредување на националните капацитети за истражување на сајбер криминалот.
11. Активно учество во креирањето на меѓународни регулативи и стандарди за сајбер криминал и нивно имплементирање на национално ниво.
12. Континуирана процена на соодветноста и ефективноста на националната регулатива за сајбер криминал.
13. Континуирана едукација на правосудните органи во областа на сајбер безбедност, сајбер криминал и електронски докази.

## ЦЕЛ 4: Сајбер одбрана

*Република Македонија да ги зајакне своите капацитети за одбрана на националните интереси и да ги намали моменталните и идните ризиците во сајбер просторот.*

За ефективно справување со ризиците во сајбер просторот, Република Македонија дефинира капацитети за сајбер одбрана по највисоки стандарди, како составен дел од националната рамка за сајбер безбедност. Развојот на способностите за сајбер одбрана во Армијата на Република Македонија е дел од севкупната национална одбрана во државата. Ова се обезбедува со вклучување на експерти од одбранбениот и безбедносниот сектор во сите работни групи и тела за справување со сајбер закани.

Еден од условите за формирање на ефикасна национална сајбер одбрана е сите организации кои нудат услуги во сајбер просторот континуирано да ги усогласуваат оперативните планови за одбрана од сајбер закани во согласност со националните сценарија, со цел заштита на КИИ и ВИИ.

Цивилно-воената соработка на меѓународно ниво се базира на ресурсите со кои располага државата и кои функционираат соодветно и во сајбер просторот - во однос на предупредувањето, превенцијата, заштитата, одвраќањето, детекцијата и активната одбрана.

Република Македонија, како земја Партнер и кандидат за членство на НАТО, Европската Унија и други меѓународни воени и цивилни организации, за да се вклучи во колективната одбрана, потребно е во целост да ги следи стандардите и насоките на овие организации и да ги искористи ресурсите и можностите кои ги нудат овие организации за развој и имплементација на заеднички сајбер безбедносни капацитети, стандарди и обуки. Во системите за колективна одбрана, Република Македонија ќе соработува и разменува информации со овие организации на полето на сајбер одбраната.

## **Активности:**

1. Дефинирање на националните капацитети за сајбер одбрана.
2. Дефинирање на воени капацитети во Министерството за одбрана и Армијата за справување со закани во сајбер просторот.
3. Формирање, развој и одржување на дефинираните капацитети и способности за сајбер одбрана.
4. Воспоставување на систем за сајбер одбрана на националната критичната инфраструктура.
5. Креирање единствена и сеопфатна правна рамка за сајбер одбрана, земајќи ја предвид позитивната законска регулатива во РМ и директивите од НАТО и ЕУ.
6. Одбрана и намалување на ризиците во сајбер просторот.
7. Воспоставување и одржување на взаемна меѓународна соработка за одвраќање на споделените сајбер закани и зголемување на националната и меѓународната безбедност и стабилност.
8. Дефинирање и координација на военото планирање за начинот и употребата на воените сајбер капацитети со националната сајбер одбрана во разни ситуации.
9. Вклучување и придонес во колективната сајбер одбрана преку меѓународна соработка.
10. Континуирана едукација за обезбедување на високо ниво на свесност и лична одговорност во однос на сајбер одбраната и националната одбрана и безбедност.
11. 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.

## ЦЕЛ 5: Соработка и размена на информации

*Република Македонија да го штити својот сајбер простор преку соработка и размена на информации на национално и меѓународно ниво, со цел да обезбеди отворен, слободен, доверлив и безбеден сајбер простор.*

Секоја организација и поединец треба самостојно да се грижи за начинот и одговорноста во користењето на најновите технологии. Сепак, доколку сакаме да имаме безбеден сајбер простор на национално ниво потребно е да се дефинираат ефикасни и ефективни процедури за соработка и размена на информации помеѓу сите засегнати страни. На овој начин би се овозможил транспарентен и безбеден начин на употреба на ИКТ. Од оваа причина, потребно е да се зајакнат капацитетите, процедурите и процесите помеѓу засегнатите страни преку постојана соработка.

Меѓународната соработка е еден од клучните сегменти во заложбите за зголемување на капацитетите за справување со заканите во сајбер просторот. Во голем дел од случаите, Република Македонија би се соочила со сајбер напади кои се делумно или во целост организирани и реализирани од злонамерни корисници кои се надвор од физичките граници на нашата држава. Во овој случај, успехот на преземените мерки за намалување на ефектите на регистрираните сајбер инциденти и пронаоѓање и преземање соодветни мерки против сторителите на кривичното дело во основа зависи од воспоставената соработка на билатерално, регионално и меѓународно ниво. Со цел да се обезбеди целосна оперативност на државните институции и надлежните органи одговорни за справување со ризиците и инцидентите во сајбер просторот потребни се интернационални партнерства на тие институции со други држави и организации. Република Македонија мора да ги преземе сите неопходни мерки да биде препознаена како држава која се грижи за безбедноста во сопствениот сајбер простор и дека сака активно да се вклучи во глобалната борба за справување со масовната злоупотреба на сајбер просторот од страна на злонамерните корисници. Активното меѓународно учество во справување



со глобалниот предизвик од сајбер заканите ќе придонесе за зголемување на државните капацитети за справување со сајбер ризиците.

#### Активности:

1. Промовирање на управување со Интернетот и норми на однесување на државата што ги одразуваат интересите на Република Македонија.
2. 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.
3. Развој на постојни и градење нови мрежи на оперативна национална, билатерална, регионална, меѓународна соработка.
4. Активно учество и давање придонес кон меѓународната способност за сајбер безбедност и јакнење на довербата.
5. Ефикасна размена на информации помеѓу државата и субјектите кои управуваат со КИИ и ВИС.
6. Поддршка во искористувањето на економските можности на сајбер просторот за населението во Република Македонија.
7. 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.
8. Соработка на засегнатите страни на истражувачки проекти на национално и меѓународно ниво.
9. Организација и учество на разни меѓународни активности и иницијативи од областа на сајбер безбедноста.
10. Воспоставување механизми и процедури за меѓународна соработка на дипломатско ниво во случај на сајбер инциденти, напади и кризи, согласно утврдените принципи на меѓународно ниво.

11. Промовирање и унапредување на нормите, правилата и принципите на одговорно однесување од страна на државата, согласно утврдените принципи на меѓународно ниво.
12. Воспоставување и унапредување на соработката и градење доверба со други меѓународни јавни и приватни CERT и CSIRT тимови, академски заедници и други меѓународни организации.
13. 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.
14. 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.
15. 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.
16. Градење на доверба помеѓу сите засегнати страни, вклучувајќи и создавање на национална платформа/систем за размена на информации во врска со закани, инциденти и непосредните опасности.

## Имплементација

По усвојувањето на Националната стратегија за сајбер безбедност, во рок од три месеци се развива Акциски план за имплементација на целите и активностите дефинирани во Стратегијата. Органите надлежни за имплементацијата на предвидените цели и активности се дефинирани согласно оваа Стратегија. Имплементацијата на мерките од стратегијата ќе бидат координирани од Националниот совет за сајбер безбедност. Во согласност со стратегијата, надлежните министерства и институции ќе спроведат анализа на легислативата и по потреба ќе извршат усогласување на регулативите процедурите во својот ресор. Надлежните министерства ќе доставуваат периодични извештаи за имплементација до Националниот совет за сајбер безбедност. Зависно од укажаната потреба, Стратегијата за сајбер безбедност може да се ревидира и ажурира.

За таа цел, Република Македонија ќе воспостави **Национален совет за сајбер безбедност** и **Тело со оперативни капацитети за сајбер безбедност**.

### Национален совет за сајбер безбедност

Со цел координација и мониторинг на спроведените активности согласно Стратегијата за сајбер безбедност, Акцискиот план, како и дефинирање на нови стратешки насоки и препораки врзани со сегментот на сајбер безбедност, Владата на Република Македонија ќе воспостави Национален совет за сајбер безбедност кој ќе има активности во насока на:

- Систематски мониторинг и координација на имплементација на Националната стратегија за сајбер безбедност и разгледување на сите предизвици во областа на сајбер безбедноста.
- Предложување конкретни мерки за подобрување на имплементацијата на Стратегијата и Акцискиот план за имплементација на Стратегијата за сајбер безбедност.

- Предлага дополнување и измени на Стратегијата и Акцискиот план со цел поефикасно справување со новите предизвици во областа на сајбер безбедноста.
- Идентификување на предизвиците за управување со сајбер кризи и предлагање соодветни мерки за поголема ефикасност.
- Учество, координација и усогласување со активностите на Советот за безбедност на Република Македонија.
- Анализа на моменталната безбедносна состојба врз основа на добиените извештаи од телото со оперативни капацитети за сајбер безбедност.
- Одобрување на планот на мерки и активности за реакција во случај на сајбер криза, предложен од телото со оперативни капацитети за сајбер безбедност.
- Развој на програми и акциски планови за активностите во областа на сајбер безбедноста кои треба да се преземат од страна на телото со оперативни капацитети за сајбер безбедност.

## Тело со оперативни капацитети за сајбер безбедност

Телото со оперативни капацитети за сајбер безбедност може да се формира како новоформиран самостоен орган (агенција, дирекција) или како новоформирана организациска единица, односно орган во рамки на постоечки орган.

Телото со оперативни капацитети би имало надлежност за операционализација на идентификуваните активности кои се дефинирани во Стратегијата и Акцискиот план за сајбер безбедност и насоките и препораките дадени од страна на Националниот совет за сајбер безбедност, со основни надлежности:

- Развој и давање препораки, мислења, извештаи, истражувања и насоки, поврзани со имплементацијата на Стратегијата за сајбер безбедност, Акцискиот план и останатите стратешки документи поврзани со сајбер безбедноста.

- Мониторинг на трендовите во безбедноста на сајбер просторот со цел детектирање закани кои можат да резултираат во сајбер криза.
- Изработка и споделување на периодични проценки за состојбата во областа на сајбер безбедноста.
- Континуирана соработка и размена на информации за сајбер закани, ранливости, инциденти, ризици и статистики за работење со сите засегнати страни.
- Предлагање план на мерки и активности за реакција во случај на сајбер криза.
- Предлагање, спроведување и учество во национални и меѓународни вежби во областа на сајбер безбедноста.
- Развивање капацитети за оперативна асистенција на ентитетите при справување со напади од поголеми размери.
- Евидентирање на моменталната состојба на ИКТ на секоја засегната страна (корисник на услугите на ова тело) и доставување редовни извештаи за настанатите промени или инциденти регистрирани од сите ентитети со цел превентивно алармирање за можните злоупотреби на тие системи.
- Мониторинг на имплементацијата на активностите предвидени со Стратегијата за сајбер безбедност и други стратешки документи и меѓународни стандарди, од страна на сите засегнати страни (корисници) на услугите на телото со оперативни капацитети за сајбер безбедност.
- Координативни и консултативни активности при имплементација на нови ИКТ решенија и развој на софтверски решенија кај сите засегнати страни (корисници) на услугите на ова тело.

## Предизвици за имплементација

Најголеми предизвици при имплементација на Стратегијата за сајбер безбедност можат да бидат ниското ниво на свесност за важноста на сигурен сајбер простор, недостатокот на сајбер хигиена, како и недостатокот на политичка волја и консензус за систематски пристап во надминување на предизвиците поврзани со сајбер безбедноста. Несистематскиот пристап може да предизвика штетни последици за државата, посебно во случај кога општеството се соочува со напредни сајбер напади од поголем размер.

Воспоставувањето на ефективна соработка меѓу засегнатите страни е исто така еден од поголемите предизвици при имплементација на Стратегијата. Соработката во областа на сајбер безбедноста во многу случаи за некои јавни чинители е нова и бара промена на навиките. Главен предизвик во делот на соработката се различните интереси и надлежности на различни засегнати страни.

Дополнително на претходно споменатото, довербата помеѓу јавниот и приватниот сектор може да биде една од главните пречки во ефективна имплементација на Стратегијата за сајбер безбедност. Воспоставувањето на доверба е процес кој бара дијалог, како и дополнително одвоено време и напор. Поради недовербата, одредени институции и организации не се подготвени да пријават безбедносни инциденти, пред сè поради потенцијална загуба на репутацијата. Недостатокот на размена на информации и отсуство на обврска за пријавување на инциденти води кон недоволна свесност за моменталната ситуација со сајбер заканите, што може да биде причина за потешкотии при реализација на активности за спротивставување на веќе познати предизвици во сајбер просторот.

Голем предизвик при имплементација на Стратегијата за сајбер безбедност на Република Македонија може да биде и недостигот на финансиски ресурси и квалификуван кадар за справување со предизвиците во сајбер просторот.

Успешната имплементација на Стратегијата за сајбер безбедност ќе има позитивно влијание на зголемена сајбер безбедност и на тој начин обезбедување на

националната безбедност. Дополнително на тоа, обезбедувањето на сајбер просторот ќе ја зголеми довербата на корисниците во сајбер просторот, што може да има значителен придонес во развојот на нови интернет базирани услуги и истото да предизвика зголемен економски раст во Република Македонија.

# АНЕКС 1

## Дефиниции

**Ботнет** - мрежа на приватни компјутери заразени со злонамерен софтвер и групно контролирана без знаење на сопствениците

**Граѓански организации** - секое здружение, фондација, сојуз, како и секој организационен облик на странска организација, како и друга форма на здружување, регистрирани согласно со одредбите на Законот за здруженија и фондации, но и неформални граѓански движења или групи на граѓани кои се занимаваат со иницијативи од областа на заштитата на човековите права и слободи.

**Задна врата (Backdoor)** – техника во која безбедносниот механизам на системот се заобиколува незабележливо, со цел да се обезбеди пристап до информациски систем или неговите податоци.

**Злонамерен софтвер (Malware)** - софтвер кој 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, како што се производство, контролирање на производството и контрола на дистрибуцијата преку програмски логички контролери кои се различни од конвенционалните информатички технологии.

**Интернет** - глобална компјутерска мрежа која обезбедува поврзување на информациски и комуникациски уреди и системи поврзани со користење стандардизирани комуникациски протоколи.

**Информациска безбедност** - состојбата на доверливост, интегритет и достапност на информации, постигната со примена на соодветни безбедносни мерки.



**Информациски системи** - Системи вклучени во обезбедувањето на било која услуга, трансакција и информации / податоци преку ИКТ.

**Класифицирана информација** - информација која се заштитува од неовластен пристап или употреба и која се определува со степен на класификација.

**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).

**Криптовалути** – децентрализирани виртуелни валути, базирани на математички принципи и заштитени со криптографски алгоритми, при што принципите на криптографијата се користат за имплементација на дистрибуирана, децентрализирана, безбедна информациска економија.

**Личен податок** - секоја информација која се однесува на идентификувано физичко лице или физичко лице кое може да се идентификува, а лице кое може да се идентификува е лице чиј идентитет може да се утврди директно или индиректно, посебно врз основа на матичен број на граѓанинот или врз основа на едно или повеќе обележја специфични за неговиот физички, физиолошки, ментален, економски, културен или социјален идентитет;

**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 кои 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.

**Национална безбедност** – систем за современ облик на организирање и функционирање на општеството заради спроведување на 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.

**Ransomware** – тип на злонамерен софтвер дизајниран да го блокира пристапот до информацискиот систем или до податоци складирани во тој систем, најчесто преку криптирање, при што се изнудува одредена сума на пари од жртвата на која за возврат и се нуди можност за декриптирање на информацискиот систем или податоците.

**Свест** - се однесува на безбедносната свест на сите лица кои споделуваат одговорност за безбедноста на информациите.

**Сајбер безбедност** - активности и мерки за заштита на информациските системи кои го формираат сајбер просторот од напади, обезбедување доверливост, интегритет и достапност на информации и системи, откривање на напади и сајбер безбедносни инциденти, активирање на механизми за контра-одговор и обновување на системите до состојба во која се наоѓале пред сајбер инцидентот.

**Сајбер војна** - акт на војна во и околу виртуелниот простор со средства кои се доминантно поврзани со информатичката технологија.

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

**Сајбер инцидент** - еден или повеќе настани поврзани со сајбер безбедноста кои предизвикуваат повреда на доверливост, интегритет или достапност на информациите и ја нарушуваат безбедноста на информацискиот систем.

**Сајбер криза** - настан или настани во сајбер просторот кои би можеле да предизвикаат или веќе предизвикале значително нарушување во општествениот, политичкиот и економскиот живот на Република Македонија. Ваквата ситуација може да влијае на безбедноста на граѓаните, демократскиот систем, политичката

стабилност, економијата, животната средина и другите национални вредности, односно националната безбедност и одбраната воопшто.

**Сајбер криминал** – опфаќа противправни активности кои се вршат во сајбер просторот, односно криминал кој може да се изврши само преку користење на ИКТ уреди и системи, каде што уредите и системите или се користат како средства за извршување на криминал, или се примарни цели на криминалните активности; или криминал овозможен од сајбер просторот, како што се традиционалните криминални активности и материјали за злоупотреба на деца, што се зголемува со сè поголемото користење на компјутерите, компјутерските мрежи или други форми на ИКТ.

**Сајбер простор** – простор во кој се остварува комуникацијата помеѓу информациските системи. Во контекст на Стратегијата, оваа дефиниција го опфаќа Интернетот и сите информациски системи поврзани со него, како и независни информациски систем.

**Сајбер напад** - операции кои 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 прилагоди, издржи и брзо да закрепне од пореметувања што произлегуваат од намерни напади, несреќи или природни закани или инциденти во сајбер просторот.

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

**Сајбер саботажа** – сајбер напад насочен против интегритетот и достапноста на ИКТ системите.

**Сајбер хигиена** - референца за практиките и чекорите што корисниците на информациските уреди и системи треба да ги преземаат за да го одржат здравјето на системот и да ја подобрат безбедноста на интернет.

**Сајбер шпионажа** – сајбер напад насочен против доверливоста на ИКТ системите.

**CERT** - се однесува на итен тим кој ќе ги спречи заканите и ќе ги обнови ИКТ системите ако се појават безбедносни инциденти. Во основа, CERT/CSIRT/CIRT обезбедува услуги за одговор во итни ситуации, превентивни услуги и управување со квалитетот на безбедноста. Мрежата на CERT се истите луѓе кои работат на сајбер безбедноста. Јакнење на една служба за сајбер безбедност и сајбер инциденти.

## АНЕКС 2

### Акроними

**ИКТ** – Информациско-комуникациски технологии

**EGDI** – Индекс за развој на е-влада

**GCI** – Глобален индекс за сајбер безбедност

**IDI** – Индекс за развој на ИКТ

**NRI** – Индекс за подготвеност на мрежите

**КИИ** - Критичната информациска инфраструктура

**ВИС** – Важни информациски системи

**DoS** – Одбивање на услуга

**DDoS** – Дистрибуирано одбивање на услуга

**CERT** – Тим за одговор на компјутерски вонредни ситуации

**CIRT** – Тим за одговор на компјутерски инциденти

**CSIRT** – Тим за одговор на инциденти врз компјутерската безбедност

**SCADA** – надзорна контрола и собирање податоци

**ЕУ** – Европска Унија

**НАТО** – Организација на Северноатланскиот договор

**МКД-ЦИРТ** - Национален центар за одговор на компјутерски инциденти

### **Учесници во изработка на документот:**

Димитар Манчев	Министерство за информатичко општество и администрација
Солза Ковачевска	Министерство за информатичко општество и администрација
Ана Малцева	Министерство за информатичко општество и администрација
Марјан Стоилковски	Министерство за внатрешни работи
Наталија Вељаноска	Министерство за внатрешни работи
Јане Стојанов	Министерство за внатрешни работи
Аленка Ѓорѓиева	Министерство за одбрана
Митко Богданоски	Министерство за одбрана
Филип Стојковски	Министерство за одбрана
Орхан Исмаили	Министерство за одбрана
Јована Ѓорѓиоска	Министерство за информатичко општество и администрација
Елена Манчева	Министерство за информатичко општество и администрација