СОБРАНИЕ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
ПАРЛАМЕНТАРЕН ИНСТИТУТ

ЗАКОНСКА РАМКА ЗА БЕЗБЕДНОСТА НА МРЕЖИТЕ И ИНФОРМАЦИСКИТЕ СИСТЕМИ ВО ЕВРОПСКАТА УНИЈА И РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

-тематска анализа-

Лидија Поповска
Истражувач и аналитичар по правосудство и фундаментални права

Декември, 2023 година

СОДРЖИНА

РЕЗИМЕ

Оваа тематска анализа го опфаќа законодавниот дел за кибербезбедноста на мрежите и информациските системи во Европската Унија и Република Северна Македонија. Во ЕУ, првата Стратегија за кибербезбедност е донесена 2013 година со пет стратешки приоритети: Постигнување на киберотпорност; Намалување на компјутерскиот криминал; Развивање политика и способности за кибердобрана; Развивање на индустриски и технолошки ресурси за кибербезбедност; и Воспоставување на кохерентна меѓународна политика за киберпросторот за Европската Унија и промовирање на основните вредности на ЕУ. Во 2020 година донесена е нова Стратегија, со конкретни предлози за унапредување во три области и тоа: Отпорност, технолошки суверенитет и лидерство; Градење оперативни капацитети за спречување, одвраќање и реагирање; и Унапредување на глобален и отворен киберпростор.

Актот за безбедност на мрежи во ЕУ е донесен 2019 година. Но, сепак, Директивата за безбедносни мрежи и информациски системи (Директива ЕУ 2016/1148) или *Директива НИС од 2016 година, претставува прв законодавен дел за кибербезбедност* чија цел е да обезбеди високо ниво на безбедност на мрежни и информациски системи. Директивата исто така наметува обврска земјите членки да ја транспонираат истата во националните законодавства најдоцна до месец мај 2018 година. Сепак, во месец декември 2020 година, Европската комисија усвојува предлог за ревидирање на Директивата НИС. Со новата Директива НИС 2 (2022/2555), се проширува опсегот на актуелната НИС Директива, со обврска земјите членки да ја транспонираат истата во нивното национално законодавство најдоцна до октомври 2024 година. Заради транспонирање на НИС Директивата во нашето законодавство, Министерството за информатичко општество и администрација, во 2019 година изработи Нацрт на предлог-закон за безбедност на мрежи и информациски системи. Потребата од носење на Законот произлегува од суштинската улога на мрежата и информациските системи, а пред сè интернетот. Додека, предмет на Законот би биле: донесување на План за дигитална трансформација на јавниот сектор во Република Северна Македонија; донесување на Национална стратегија за кибербезбедност; Определување на надлежно тело за безбедност на мрежни и информациски системи и дигитална трансформација на јавниот сектор и утврдување на неговите надлежности; Управување со киберкризи, единствена точка за контакт за безбедност на мрежни и информациски системи, како и национално тело за одговор на компјутерски инциденти, и друго. Во РСМ исто така, донесена е Национална стратегија за сајбер безбедност 2018-2022 година, која всушност претставува прва стратегија од оваа област во нашата држава. Во моментот постои Документ за дискусија - Национална стратегија за сајбер безбедност од 2023 до 2026 година, кој во иднина би се третирал како новата стратегија. Во поглед на кибердобраната Министерството за одбрана има донесено Национална стратегија за сајбер одбрана и Акциски план за имплементација за период од 2019-2023 година.

ВОВЕД

Со појавата на интернетот и неговата се поголемата употреба, неопходно е да се проценат безбедносните ризици и справувањето со нив. Сегашното информатичко доба ги постави информациите и кибербезбедноста во преден план како важни аспекти на индивидуалната, организациската, државната и меѓународната безбедност. Карактеристики на кибербезбедноста се: зачувувањето на доверливоста, интегритетот и достапноста на информациите.

Во концептот на доброто управување со безбедносниот сектор, безбедносните политики имаат за цел не само осигурување на безбедноста на државата, туку и безбедноста на поединецот. Примената на овој пристап кон интернетот значи дека кибербезбедноста треба да се стреми кон креирање на безбеден интернет простор за сите. За да се постигне ова, политиката за кибербезбедност мора да покрива голем број прашања, од заштитата на државниот интегритет и гарантирањето на човековите права, до спроведувањето на законите и спречувањето на кривични дела извршени во, или со користење на киберпросторот. Според тоа, прашањата на управувањето со кибербезбедноста треба не само да одговорат на прашањето за одржување на безбедноста и отпорноста на интернет, туку и на градењето безбедност и поттикнувањето можности на интернет[1].

I Регулативи за кибербезбедноста во ЕУ

I.1 Стратегии за кибербезбедност на ЕУ

Од страна на институциите на Европската Унија во 2013 година, заеднички е објавена **Стратегија за кибербезбедност на Европската Унија: Отворен, безбеден и сигурен киберпростор**[2].

Визијата на Европската Унија претставена во оваа Стратегија е систематизирана во пет стратешки приоритети и тоа:

- Постигнување на киберотпорност;
- Драстично намалување на компјутерскиот криминал;
- Развивање политика и способности за кибероодбрана поврзани со заедничката безбедност и одбранбена политика;
- Развивање на индустриски и технолошки ресурси за кибербезбедност;
- Воспоставување на кохерентна меѓународна политика за киберпросторот за Европската Унија и промовирање на основните вредности на ЕУ[3].

Во 2020 година ЕУ објавува нова Стратегија за кибербезбедност, пред сè поради неопходноста да се направи друг чекор за изградба на построга и поцврста стратегија. Без разлика дали се работи за поврзани уреди, електрични мрежи или банки, авиони, јавна администрација или болниците што ги користат

[1] Вовед во управувањето со кибербезбедност - Прирачник за пратеници, стр.5 https://www.dcaf.ch/sites/default/files/publications/documents/CyberPolicyToolMACEDONIAN%28Cyrillic%29.pdf
[2]Стратегија за кибербезбедност од 2013 година https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN
[3] *Ibid*

или ги посетуваат, луѓето заслужуваат гаранцијата дека ќе бидат заштитени од киберзакани. Економијата, демократијата и општеството на ЕУ зависат повеќе од кога било од безбедни и доверливи дигитални алатки и поврзување.

Новата Стратегија содржи конкретни предлози за распоредување на регулаторни, инвестициски и политички инструменти за решавање на три области и тоа:

- Отпорност, технолошки суверенитет и лидерство;
- Градење оперативни капацитети за спречување, одвраќање и реагирање;
- Унапредување на глобален и отворен киберпростор[4].

I.2 Акт за кибербезбедност на ЕУ

Во 2019 Европската унија објавува нова Регулатива 2019/881 наречена **Акт за кибербезбедност.** За да се обезбеди правилно функционирање на внатрешниот пазар, а истовремено да се постигне високо ниво на кибербезбедност, киберотпорност и доверба во Унијата, оваа Регулатива утврдува:

- цели, задачи и организациски прашања кои се однесуваат на ЕНИСА (Агенција на Европската Унија за кибербезбедност); и
- рамка за воспоставување на европски шеми за сертификација на кибербезбедноста со цел да се обезбеди соодветно ниво на кибербезбедност за ИКТ (Информатичко Комуникациска Технологија) производи, ИКТ услуги и ИКТ процеси во Унијата, како и со цел да се избегне фрагментација на внатрешниот пазар во однос на шемите за сертификација на кибербезбедноста во Унијата.

Агенцијата на Европската Унија за Мрежна и информациска безбедност (ЕНИСА) ќе игра одлучувачка улога во процесот на сертификација[5]. Целта на Агенцијата е да се постигне високо заедничко ниво на кибербезбедност низ Унијата, преку активна поддршка на земјите членки, институциите, телата, канцеларииите на Унијата и агенциите за подобрување на кибербезбедноста. Агенцијата дејствува како референтна точка за совети и експертиза за кибербезбедноста, и придонесува за намалување на фрагментацијата на внатрешниот пазар. При извршувањето на своите задачи, Агенцијата дејствува независно, избегнувајќи дуплирање на активностите на земјите членки и земајќи ја предвид постојната експертиза од земјите членки[6]. Агенцијата би се финансирала од: Придонес од општиот буџет на Унијата; Приходи наменети за одредени расходни ставки; Финансирање од Унијата во форма на договори за делегирање или ад хок грантови; Придонеси од трети земји кои учествуваат во работата на ЕНИСА; и Сите доброволни придонеси од земјите-членки со финансиски или нефинансиски придонес[7].

[4] Стратегија за сајбер безбедност на ЕУ од 2020 година https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=ga
[5]Cybersecurity Act, Article1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN
[6] *Ibid* Article 3
[7] *Ibid* Article 30

I.3 Директива НИС (преглед)

Европскиот парламент и Советот на Европска Унија во месец јули 2016 година, ја усвојуваат **Директива за безбедносни мрежи и информациски системи** (Директива ЕУ 2016/1148) **или „Директива НИС“**, која стапува на сила во месец август истата година[8]. *Директивата НИС всушност претставува прв законодавен дел за кибербезбедност, чија цел е да обезбеди високо ниво на безбедност на мрежни и информациски системи.* Директивата исто така наметува обврска земјите членки да ја транспонираат истата во националните законодавства најдоцна до месец мај 2018 година, но и да ги идентификуваат операторите на основните услуги (ОЕС) со основање на нивната територија, најдоцна до 2018 година.

Пред усвојување на Директивата НИС, земјите членки на ЕУ имале различни нивоа на подготвеност за кибербезбедност, поради што постојните капацитети не биле доволни да се обезбеди високо ниво на безбедност на мрежните и информациските системи во ЕУ. Оттука, поради недостатокот на **идентификувани оператори на основните услуги (ОЕС), но и на давателите на дигитални услуги,** се јавува нееднаква заштитеност на потрошувачите и на бизнисите, како резултат на што било оневозможено воспоставување на хармонизиран глобален и ефективен механизам за соработка на ниво на ЕУ.

Главни цели на Директивата НИС се:

- Подобрување на националните способности за кибербезбедност преку спроведување на Национална стратегија;
- Градење соработка на ниво на ЕУ; и
- Промовирање на култура на управување со ризик и известување за инциденти за идентификуваните даватели на основните услуги (ОЕС) и давателите на дигиталните услуги (ДПС).

Сепак, во месец декември 2020 година, Европската комисија усвојува предлог за ревидирање на Директивата НИС. Поконкретно, предлогот додава нови сектори врз основа на нивната критична природа, со што се проширува опсегот на актуелната НИС Директива, како и елиминирање на разликата помеѓу давателите на дигитални услуги и операторите на основните услуги. Дополнително, предлогот се однесува на посилен синџир на обезбедување на кибербезбедност и попрецизни одредби за управување со ризик и известување за инциденти.

Во месец октомври 2021 година, Комитетот за индустрија, истражување и енергија на Европскиот парламент (ИТРЕ) усвојува извештај за Директивата НИС 2, како и мандатот да влезе во меѓуинституционални преговори. Извештајот вклучува построги обврски за кибербезбедноста во однос на управувањето со ризикот, обврските за известување и споделувањето информации, се обидува да го намали административниот товар и да го подобри известувањето за инциденти за кибербезбедноста. Дополнително, извештајот повикува на построги мерки за надзор и спроведување низ земјите членки и има за цел

[8] Directive (EU) 2016/1148 of the European Parlament and of the Council of 6 July 2016 (Directive NIS), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016L1148&from=EN , пристапено на ...

дополнително да го прошири опсегот на Директивата НИС 2 со вклучување на академски, научни и истражувачки институции.

Понатаму, во месец декември 2021 година Советот на ЕУ, објавува дека го усвоил својот општ пристап за Директивата НИС 2[9].

Директивата НИС 2 (2022/2555), е објавена во Службениот весник на Европската унија во декември 2022 година, а стапува на сила во јануари 2023 година. Согласно одредбите од Директивата НИС 2, земјите-членки мора да ја транспонираат Директивата НИС 2 во нивното национално законодавство најдоцна до 17 октомври 2024 година, а законите за транспонирање ќе се применуваат од 18 октомври 2024 година. На истиот датум, Директивата НИС (2016/1148) ќе престане да важи[10].

Со транспортирањето на Директивата НИС во националните законодавства на земјите членки, пред сè, би се обезбедил усогласен глобален и ефективен механизам за соработка за идентификувани оператори на основните услуги (ОЕС), но и на давателите на дигитални услуги (ДСП), како и способност земјите членки ефикасно да одговорат на предизвиците на безбедноста на мрежа и информациски системи. Оттука, согласно Директивата, произлегува обврската земјите членки да назначат еден или повеќе тимови за одговор на инциденти од компјутерска безбедност (CSIRT), а задачите на **CSIRT** би вклучувале:

- Следење на инциденти на национално ниво;
- Обезбедување рано предупредување, предупредувања, соопштенија и дисеминација на информации до релевантните засегнати страни за ризици и инциденти;
- Реагирање на инциденти;
- Обезбедување динамична анализа на ризик и инциденти и ситуациона свест; и
- Учество во мрежата CSIRTs.

Притоа, земјите членки може да побараат помош од **Агенцијата за киберезбедност на Европската Унија (ЕНИСА) во развојот на националните CSIRT[11]**.

Понатаму, следна обврска на земјите членки е да соработуваат преку Групата за соработка формирана со Директивата НИС, со цел да се поддржи и олесни стратешката соработка и размената на информации меѓу земјите-членки и да се развие и довербата меѓу нив. Групата за соработка мора да биде составена од претставници на земјите членки, Комисијата и ЕНИСА. За Групата за соработка да биде ефективна и инклузивна, од суштинско значење е сите земји членки да имаат минимум способности и стратегија што обезбедува високо ниво на безбедност на мрежните и информациските системи на нивната територија. Главните задачи на Групата за соработка се следните:

- обезбедување стратешки насоки за активностите на мрежата CSIRTs; и

[9] Интернетска страница на Европска комисија https://www.dataguidance.com/opinion/eu-overview-nis-directive

[10] Directive (EU) 2022/2555 of the European Parlament and of the Council of 14 December 2022 (Directive NIS 2), Official Journal of the European Union L 333/80 from 27.12.2022 https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[11] Интернетска страница на Европска комисија https://www.dataguidance.com/opinion/eu-overview-nis-directive

- размена на информации и најдобри практики за подигање на свеста и обука.

Најпосле, обврска на земјите членки е да назначат:

- еден или повеќе национални надлежни органи за безбедноста на мрежата и информациските системи за следење на примената на Директивата НИС на национално ниво; и

- единствена точка на контакт („SPOC“) за вршење на функцијата за врска, со цел да се обезбеди прекугранична соработка помеѓу органите на земјите-членки и релевантните органи во другите земји-членки, како и со Групата за соработка и мрежата CSIRT наведени погоре.

Во случај на неусогласеност во однос на горенаведеното, Директивата ги обврзува земјите членки да утврдат правила за казни што ќе се применуваат за прекршување на националните одредби усвоени во согласност со Директивата, но и да ги преземат сите неопходни мерки за да се осигурат дека тие се имплементирани. Притоа, казните мора да бидат ефективни, пропорционални и одвраќачки[12].

II Преглед на преземени чекори во однос на имплементацијата на европската регулатива за кибербезбедност во Република Северна Македонија

II.1 Нацрт на предлог-закон за безбедност на мрежи и информациски системи

МИОА заради транспонирање на НИС Директивата во нашето законодавство, во 2019 година, изработи **Нацрт на предлог-закон за безбедност на мрежи и информациски системи**. Во Извештајот од МИОА кој се однесува на проценката на влијанието на законската регулативата, направен е опис на состојбата во Северна Македонија во полето на безбедноста на мрежните и информациските системи. Според овој Извештај, потребата од носење на Законот произлегува од суштинската улога на мрежата и информациските системи, а пред сè интернетот, во однос на олеснувањето на прекугранично движење на стоки, услуги и луѓе. Оттука, поради таа транснационална природа, значителни нарушувања на овие системи без разлика дали се намерни или ненамерни и без оглед каде се случуваат, може да влијаат и врз нашата држава. Затоа, безбедноста на мрежните и информациските системи е од суштинско значење за непречено функционирање на внатрешниот пазар. Потребата за носење на овој закон, исто така се наметнува и поради фактот што во РСМ отсуствува правна регулатива во оваа област. Дополнително, со Законот би се транспонирала Директивата (ЕУ) 2022/2555 на Европскиот парламент и на Советот од 14 декември 2022 година во однос на мерките за високо заедничко ниво на кибербезбедност низ Унијата, односно НИС 2 Директивата[13].

[12]Интернетска страница на Европска комисија https://www.dataguidance.com/opinion/eu-overview-nis-directive

[13] Интернетска страница на ЕНЕР, Нацрт Извештај за проценка на влијанието на регулативата Предлог на Закон за безбедност на мрежи и информациски системи,

II.1.1 Што содржи Нацртот?

Пред се, предмет на Нацрт-законот за безбедност на мрежи и информациски системи би биле: донесување на План за дигитална трансформација на јавниот сектор во Република Северна Македонија; донесување на Национална стратегија за кибербезбедност; определување на надлежно тело за безбедност на мрежни и информациски системи и дигитална трансформација на јавниот сектор и утврдување на неговите надлежности; управување со киберкризи, единствена точка за контакт за безбедност на мрежни и информациски системи, како и национално тело за одговор на компјутерски инциденти, и друго. Додека, **целта на** овој Нацрт-закон би било обезбедување на:

- високо ниво на кибербезбедност со цел заштита и понатамошен развој на општеството,
- градење и проширување на ИТ инфраструктурата, односно поефикасна и поефективна дигитална трансформација на јавниот сектор,
- повисок степен на отвореност со цел да се обезбеди развој на иновативни софтверски решенија,
- обуки за кибербезбедност и дигитални вештини за вработените во јавниот сектор и граѓаните на Република Северна Македонија[14].

II.1.2 Предлог за основање на Агенцијата за безбедност на мрежни и информациски системи и дигитална трансформација

Со овој Нацрт-закон се предлага основање на Агенцијата за безбедност на мрежни и информациски системи и дигитална трансформација, која би била надлежно тело за безбедност на мрежни и информациски системи и дигитална трансформација на јавниот сектор во Република Северна Македонија. Агенцијата би била регулаторно тело, со статус на правно лице, со јавни овластувања, а основач на Агенцијата е РСМ. Агенцијата ги извршува работите во согласност со овој закон и прописите донесени врз основа на него, Законот за општата управна постапка, Законот за административни службеници, Закон за вработените во јавниот сектор и други закони и стратешки документи на РСМ, како и препораките и насоките на Европската комисија и Агенцијата за кибербезбедност на Европската Унија (ЕНИСА)[15]. Исто така, предвиден е широк спектар на надлежности на Агенцијата[16]. За својата работа Агенцијата е одговорна пред Владата и има обврска да доставува Годишен извештај за

https://ener.gov.mk/files/propisi_files/plan/64_1223013106%D0%9D%D0%B0%D1%86%D1%80%D1%82%20%D0%98%D0%B7%D0%B2%D0%B5%D1%88%D1%82%D0%B0%D1%98%20%D0%B7%D0%B0%20%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D0%BD%D0%BA%D0%B0%20%D0%BD%D0%B0%20%D0%B2%D0%BB%D0%B8%D1%98%D0%B0%D0%BD%D0%B8%D0%B5%D1%82%D0%BE%20%D0%BD%D0%B0%20%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D0%B0.doc , пристапено на 16.10.2023.

[14] Општи одредби од Нацрт на предлог-закон за безбедност на мрежи и информациски системи, https://ener.gov.mk/files/propisi_files/ria1/53_1076159645%D0%9D%D0%B0%D1%86%D1%80%D1%82%20-%20%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD_%D0%9F%D1%80%D0%B5%D0%B4%D0%BB%D0%BE%D0%B3%20%D0%BD%D0%B0%20%D0%97%D0%B0%D0%BA%D0%BE%D0%BD%20%D0%B7%D0%B0%20%D0%B1%D0%B5%D0%B7%D0%B1%D0%B5%D0%B4%D0%BD%D0%BE%D1%81%D1%82%20%D0%BD%D0%B0%20%D0%BC%D1%80.docx

[15] *Ibid* чл.4

[16] *Ibid* чл.5 Надлежности на Агенцијата за безбедност на мрежни и информациски системи и дигитална трансформација

работа за претходната година и Годишна програма за работа за наредната година. Годишниот извештај за работа за претходната година би содржел:

- извештај за реализацијата на активностите утврдени во годишната програма за работа на Агенцијата за претходната година,
- финансиски извештај за реализација на финансискиот план за претходната година и годишна сметка, со податоци за реализирани приходи, расходи, побарувања и обврски за претходната година групирани по структура и по организациска структура на Агенцијата,
- ревизорски извештај од независен меѓународен овластен ревизор и ревизорски извештај од Државниот завод за ревизија, доколку е извршена ревизија од него, како и став на Агенцијата во однос на резултатите од извршената ревизија[17].

Во однос на **финансирањето на Агенцијата**, средствата за финансирање на оперативните трошоци на Агенцијата (плати, надоместоци, обуки, трошоци за комунални услуги, потрошен материјал, технички средства и сл.) **би се обезбедувале од Буџетот на Република Северна Македонија**, а во согласност со претходно усвоена Годишна програма за работа на Агенцијата за наредната година. Притоа, **вкупните годишни средства не може да бидат помали од 0,6% од реализираните даночни приходи утврдени во последната донесена завршна сметка на Буџетот на Република Северна Македонија**. Исто така, од Буџетот на РСМ би се издвојувале и дополнителни средства за годишни софтверски лиценци и капитални инвестиции на Агенцијата за развој на своите надлежности за кибербезбедност и дигитална трансформација, согласно овој закон. Дополнителните средства за капитални инвестиции се одобруваат врз основа на усвоена Студија за изводливост од страна на Владата. Агенција би можело да се финансира и од донации, меѓународни проекти и грантови за кибербезбедност и дигиталната трансформација. Предвидена е и ставка за враќање на средства во Буџетот, во случај кога Агенцијата нема да ги потроши обезбедените средства од Буџетот[18].

II.1.3 Применливост на Нацрт-законот

Одредбите на овој Нацрт-закон, во однос на кибербезбедноста би се применувале на органите на државната управа и правните лица на кои со закон им е доверено да вршат јавни овластувања, понатаму, на субјекти, односно правни лица со регистрирано седиште во РСМ, а кои се сметаат за средни или големи претпријатија кои обезбедуваат услуги во сектори одредени во самиот Закон, како и на правни лица без оглед на нивната големина, во случаи определени со Закон. Сепак, постојат одредени исклучоци во однос на применливоста на Законот. Така, *Законот не би се применувал на Собранието на РСМ, судовите, јавните обвинителства, државното правобранителство, Народната банка и единиците на локалната самоуправа во РСМ, како и на државните органи и правните лица на кои со закон им е доверено да вршат јавни овластувања од областа на безбедноста и одбраната на РСМ.*

Доколку пак одредени субјекти немаат регистрирано седиште во Република Северна Македонија, а се даватели на услуги за DNS, регистри на имиња на врвни домени, даватели на услуги за регистрација на имиња на домени,

[17] чл.10 од Нацрт на предлог-закон за безбедност на мрежи и информациски системи
[18] чл.24 од Нацрт на предлог-закон за безбедност на мрежи и информациски системи

даватели на услуги за компјутерска обработка во облак, даватели на услуги за податочен центар, даватели на услуги за мрежи за испорака на содржини, даватели на управувани услуги, даватели на управувани безбедносни услуги, даватели на услуга на интернет пазар, даватели на услуги на -интернет-пребарувачи или даватели на платформи за услуги за социјални мрежи, должни се да именуваат свој претставник за РСМ[19].

Нацртот на предлог-законот содржи одредби и за **дигиталната трансформација на јавниот сектор**. Оттука, дигиталната трансформација би се однесувала на органите на државната управа, освен на органите на државната управа од областа на безбедноста и одбраната на Република Северна Македонија. Сепак, дигиталната трансформација би се однесувала и на јавни институции, кои не се претходно наведени, по нивно барање, а во согласност со овој Закон и во согласност со Планот за дигитална трансформација на јавниот сектор. Со Планот би се обезбедила транзиција од дистрибуирана дигитална инфраструктура на јавниот сектор кон централизирана Владина дигитална инфраструктура, односно, миграција на информациските системи на јавниот сектор во Владин облак[20].

II.2 Национални стратегии за кибербезбедноста и одбраната во Република Северна Македонија

Во насока на развојот на правната регулатива во областа на кибербезбедноста и безбедноста на информацискиот систем, во РСМ донесена е првата Национална стратегија за сајбер безбедност за периодот од 2018 до 2022 година. Втората Национална стратегија за сајбер безбедност која би се однесувала за периодот од 2023 до 2026 година, во моментот е документ за дискусија, кој документ би се третирал како идната Стратегија. Кога станува збор за киберодбраната, од страна на Министерството за одбрана донесена е Национална стратегија за сајбер одбрана и Акциски план за имплементација за период од 2019 до 2023 година.

II.2.1 Национална стратегија за сајбер безбедност од 2018-2022 година

Национална стратегија за сајбер безбедност за период од 2018-2022 година, всушност е првата Стратегија во оваа област, и истата претставува стратешки документ за развој на сигурно, безбедно, доверливо и отпорно дигитално окружување, поддржано од квалитетни капацитети, кои се базираат на доверба и соработка во полето на кибербезбедноста. Принципи кои ја поддржуваат Стратегијата се: ефективни и ефикасни капацитети за кибербезбедност; заштита и превенција; сигурност за економски развој; доверба и достапност; и правна сигурност. Согласно Стратегијата, засегнати страни во полето на кибербезбедност се: јавен сектор; приватен сектор; академска заедница; и граѓани и граѓански здруженија.

[19] *Ibid* Глава III – Кибербезбедност
[20] *Ibid*чл.63 и 64

Основни цели на Стратегијата се следните:

- Воспоставување на ИКТ-инфраструктура отпорна на киберзакани, идентификување и имплементирање на соодветни решенија за заштита на националните интереси;
- Промовирање на култура за кибрбезбедност, со цел сеопфатно разбирање на киберзаканите, како и градење и унапредување на потребните капацитети за заштита;
- Зајакнување на националните капацитети за превенција, истражување и соодветен одговор на киберкриминалот;
- Зајакнување на капацитетите за одбрана на националните интереси и намалување на тековните и идните ризици во киберпросторот; и
- Соработка и размена на информации на национално и меѓународно ниво.

Во насока на поддршка на целите и активностите, Стратегијата ги дефинира одговорностите кои се однесуваат на органите на власта. Оттука, успешната реализација на Стратегијата подразбира оформување на Национален совет за кибербезбедност и Тело со оперативни капацитети за кибербезбедност.

Национална 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[21].

Со цел имплементација на Стратегијата, донесен е Акциски план за 2018-2022 година. По извршена анализа на капацитетите за кибербезбедност на национално ниво, оформена е работна група одговорна за развивање на стратешки документи од областа на кибербезбедноста, која вклучува претставници од трите надлежни министерства за кибербезбедност во РСМ - Министерството за информатичко општество и администрација, Министерството за одбрана и Министерството за внатрешни работи. Овој Акциски план ги вклучува главните активности потребни за зајакнување на националните капацитети за кибербезбедност, кои се поделени на активности со висок, среден и низок приоритет[22].

II.2.2 Документ за дискусија - Национална стратегија за сајбер безбедност од 2023 до 2026 година

Во месец ноември 2022 година од страна на Министерство за информатичко општество и администрација (МИОА), како надлежна институција за процесот на изработка на Националната стратегија за кибербезбедност, изготвен е документ за дискусија, кој документ би се третирал како идната Национална стратегија за сајбер безбедност за периодот од 2023 до 2026 година[23].

Според документот, новата Стратегија за сајбер безбедност, освен одржувањето на безбедноста и отпорноста на Интернетот, би требало да се

[21] Интернетска страница на Министерство за информатичко општество и администрација, Национална стратегија за национална безбедност на РМ 2018-2022 https://portal.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_sajber_bezbednost_2018-2022.pdf , пристапено на 16.10.2023.

[22] Интернетска страница на МИОА, Акциски план 2018-2022 https://portal.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/AP%20v1.13MK.pdf , пристапено на 16.10.2023.

[23] Интернетска страница на МИОА, https://obse.mioa.gov.mk/?q=en/node/4407 , пристапено на 16.10.2023.

насочи кон континуирано градење и зајакнување на киберотпорноста и безбедноста. Неодамнешните инциденти врз мрежите на нашите институции, но и на државните мрежи на соседните земји, се наведени како релевантен показател дека всушност постои огромна реална закана за сите нас. Исто така, како не помалку важни, се посочени и киберинцидентите кои често ги погодуваат семејствата и локалните бизниси, што резултира со финансиски загуби, прекин на работата, кражба на идентитетот и психолошки стрес. Оттука, за успешна стратегија, потребно е истата да се креира во партнерство и во согласност со сите засегнати страни, и тоа: мали, средни и големи бизниси, индустриските тела, академијата, невладините организации, владините агенции, групи на заедницата и членови на јавноста. Самиот документ содржи прашања, кои би биле клучни за Стратегијата, како и статистички податоци во врска со прашањата. Преку отворена дискусија по прашањата, би се слушнале ставовите на сите засегнати страни, со што би се постигнала целта на Документот, што пак од друга страна, би придонело за значителен напредок во полето на кибербезбедноста во нашата држава[24].

Табела 1: Приказ на прашања од Документот за дискусија, со статистички податоци[25]

1.	Каде сме сега?	„Во 93 % од случаите, надворешен напаѓач може да го пробие мрежното опкружување на организацијата и да добие пристап до ресурсите на локалната мрежа.“
2.	Прашања за иднината	„Важно е дефинирањето на соодветните улоги во владините установи, индустријата и заедницата.”
3.	Улогата на државата во светот што се менува	„Во 2021 година, 22 милијарди податоци биле неовластено откриени од протекувањето на податоците.“
4.	Улогата на организациите, приватниот сектор и Националните информатички системи во кибербезбедноста	„Во просек, само 5 % од податоците на компаниите се соодветно заштитени.“
5.	Свесност, обуки, вежби и добро обучени експерти за киберзакани	„43 % од сите прекршувања се инсајдерски закани, било намерни или ненамерни.“
6.	Минимизирање на влијанието на киберинциденти и киберзакани	„37% од најчести типови на малициозни прикачувања преку е-пошта се .doc и .dot, а следен најчесто користен е .exe со 19,5 %.“

[24]Документ за дискусија-Национална стратегија за сајбер безбедност 2023-2026, https://ener.gov.mk/PublicDocuments/%D0%94%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%20%D0%B7%D0%B0%20%D0%B4%D0%B8%D1%81%D0%BA%D1%83%D1%81%D0%B8%D1%98%D0%B0%20-%20%D0%9D%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D0%BD%D0%B0%20%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D0%B8%D1%98%D0%B0%20%D0%B7%D0%B0%20%D1%81%D0%B0%D1%98%D0%B1%D0%B5%D1%80%20%D0%B1%D0%B5%D0%B7%D0%B1%D0%B5%D0%B4%D0%BD%D0%BE%D1%81%D1%82%202023-2026_%D0%9D%D0%B0%D1%86%D1%80%D1%82_id=45_version=1.pdf , пристапено на 16.10.2023.

[25]*Ibid*

Исто така, Документот дава осврт и на институциите кои на некој начин го регулираат безбедносниот систем на мрежите во РСМ, и тоа:

- **Национален центар за одговор на компјутерски инциденти MKD-CIRT,** кој претставува официјална национална точка за контакт и координација во справувањето со безбедносните инциденти кај мрежите и информациските системи, а воедно идентификува и обезбедува одговор на безбедносни инциденти и ризици. Овој Центар е во состав на Агенцијата за електронски комуникации како посебна организациона единица
- **CSIRT - ФИНКИ (академски сектор)**, односно организациска единица на Факултетот за информатички науки и компјутерско инженерство, чија цел е да обезбеди детектирање, решавање и превенција во врска со безбедноста на информациите и мрежата при факултетот.
- **Министерството за информатичко општество и администрација (МИОА),** чија одговорност се сите прашања што се однесуваат на информатичката технологија, но и на политиката и стратегијата во е-Влада. Поради потребата од олеснување на активностите кои се однесуваат на отпорноста на критичната национална инфраструктура за кибербезбедноста во Северна Македонија, под надлежност на МИОА во 2021 година формирана е **работната група за кибербезбедност за критична инфраструктура (CICWG).** CICWG делува како механизам за координација на клучните чинители, форум за соработка и цел за дефинирање на критична инфраструктура, проценка на ризик, планирање на начини за ублажување/отстранување на ризици, и развој и имплементација на механизми за споделување информации.
- **Министерството за внатрешни работи (МВР)** е водечка институција за борба против киберкриминалот. За таа цел МВР има создадено единствена и сеопфатна правна рамка за компјутерски криминал, истовремено ангажирајќи се во модернизацијата на релевантните институции за ефикасна борба против компјутерскиот криминал.
- **Министерството за одбрана (МО)** е водечка институција за киберодбрана - во 2021 година, по влезот во НАТО, Северна Македонија потпиша Меморандум за разбирање со цел унапредување на соработката за киберодбрана меѓу НАТО и одбранбените власти на земјата; Меморандумот за соработка особено се фокусира на споделување информации, размена на најдобри практики и зголемување на отпорноста кон киберзаканите[26].

[26] *Ibid*

II.2.3 Национална стратегија за сајбер одбрана и Акциски план за имплементација 2019-2023 година

Како надлежен орган за киберодбраната, Министерството за одбрана има донесено **Национална стратегија за сајбер одбрана и Акциски план за имплементација за период од 2019-2023 година**. Стратегија за сајбер одбрана е развиена во согласност со Националната стратегија за сајбер безбедност, Стратегијата за кибербезбедност на Европската унија и Политиката и заложбата за кибербезбедност на НАТО за обезбедување на сигурно, безбедно, доверливо и отпорно дигитално опкружување. Визијата на Стратегијата за киберодбрана, 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 киберодбраната. Додека пак, мисијата на Стратегијата за киберодбрана е да се развијат и зајакнат капацитетите и способностите за активно следење на киберпросторот од заканите и нападите и намалување на ефектите од овие закани, со цел заштита на националните интереси. Стратегијата има четири стратешки цели, и тоа:

- **Способности за киберодбрана** - Воспоставување и одржување соодветни способности за киберодбрана со основна цел заштита на националните интереси;
- **Едукација и обука** - Градење високо квалитетен и обучен клучен персонал, како и одржување на основните принципи за киберхигиена преку константна основна обука;
- **Соработка и размена на информации** - Унапредување на соработката и размената на информации на национално и меѓународно ниво; и
- **Правна и регулаторна рамка** - Усогласување на постоечките и имплементирање нови соодветни законски регулативи, прописи и процедури за одбрана на киберпросторот и заштита на националните интереси.

Имплементацијата на Стратегијата ќе се реализира согласно Акцискиот план и ќе биде предмет на постојана годишна анализа и оценување, со конкретни предлози за унапредување[27].

III Меѓународна соработка

Во 2004 година нашата држава ја има ратификувано Будимпештанска конвенција за компјутерски криминал[28]. Будимпештанската конвенција претставува рамка која им дозволува на стотици практичари од земјите потписници, да споделуваат искуство и да создаваат односи што ја олеснуваат соработката во конкретни случаи, вклучително и во итни ситуации, надвор од специфичните одредби предвидени во оваа Конвенција. Притоа, секоја земја

[27] Национална стратегија за одбрана и Акциски план за имплементација 2019-2023 година, https://mod.gov.mk/inc/uploads/2021/06/Strategija-za-sajber-odbrana-mk-1-1.pdf , пристапено на 16.10.2023.
[28] Cybercrime Programme Office (C-PROC) of the Council of Europe https://rm.coe.int/octocom-legal-profile-nm-revised-by-nm/16809e5dd6

може да ја користи Будимпештанската конвенција како упатство, листа за проверка или модел на закон[29].

Во 2021 година, по влезот во НАТО, Северна Македонија потпиша Меморандум за разбирање со цел унапредување на соработката за киберодбрана меѓу НАТО и одбранбените власти на земјата. Меморандумот за соработка особено се фокусира на споделување информации, размена на најдобри практики и зголемување на отпорноста[30].

Изработила: Лидија Поповска
Одобрила и Согласна: Фани Коровешовска Коларовска

Раководител на Парламентарен институт

_____

Златко Атанасов

[29] https://www.coe.int/en/web/cybercrime/the-budapest-convention
[30] https://eucyberdirect.eu/atlas/country/north-macedonia/compare/european-union

ЛИСТА НА ИЗВОРИ

1. Вовед во управувањето со сајбер безбедност - Прирачник за пратеници, стр.5 https://www.dcaf.ch/sites/default/files/publications/documents/CyberPolicyToolMACEDONIAN%28Cyrillic%29.pdf
2. Стратегија за сајбер безбедност од 2013 година https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN
3. Стратегија за сајбер безбедност на ЕУ од 2020 година https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=ga
4. Cybersecurity Act, Article1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN
5. Directive (EU) 2016/1148 of the Europien Parlament and of the Council of 6 July 2016 (Directive NIS), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016L1148&from=EN
6. Интернетска страница на Европска комисија https://www.dataguidance.com/opinion/eu-overview-nis-directive
7. Интернетска страница на ЕНЕР, Нацрт Извештај за проценка на влијанието на регулативата Предлог на Закон за безбедност на мрежи и информациски системи, https://ener.gov.mk/files/propisi_files/plan/64_1223013106%D0%9D%D0%B0%D1%86%D1%80%D1%82%20%D0%98%D0%B7%D0%B2%D0%B5%D1%88%D1%82%D0%B0%D1%98%20%D0%B7%D0%B0%20%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D0%BD%D0%BA%D0%B0%20%D0%BD%D0%B0%20%D0%B2%D0%BB%D0%B8%D1%98%D0%B0%D0%BD%D0%B8%D0%B5%D1%82%D0%BE%20%D0%BD%D0%B0%20%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D0%B0.doc
8. Општи одредби од Нацрт на Предлог Закон за безбедност на мрежи и информациски системи, https://ener.gov.mk/files/propisi_files/ria1/53_1076159645%D0%9D%D0%B0%D1%86%D1%80%D1%82%20-%20%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD_%D0%9F%D1%80%D0%B5%D0%B4%D0%BB%D0%BE%D0%B3%20%D0%BD%D0%B0%20%D0%97%D0%B0%D0%BA%D0%BE%D0%BD%20%D0%B7%D0%B0%20%D0%B1%D0%B5%D0%B7%D0%B1%D0%B5%D0%B4%D0%BD%D0%BE%D1%81%D1%82%20%D0%BD%D0%B0%20%D0%BC%D1%80.docx
9. Интернетска страница на Министерство за информатичко општество и администрација, Национална Стратегија за национална безбедност на РМ 2018-2022 https://portal.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_sajber_bezbednost_2018-2022.pdf
10. Интернетска страница на МИОА, Акциски план 2018-2022 https://portal.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/AP%20v1.13MK.pdf

11. Интернетска страница на МИОА, https://obse.mioa.gov.mk/?q=en/node/4407

12. Документ за дискусија-Национална Стратегија за сајбер безбедност 2023-2026, https://ener.gov.mk/PublicDocuments/%D0%94%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%20%D0%B7%D0%B0%20%D0%B4%D0%B8%D1%81%D0%BA%D1%83%D1%81%D0%B8%D1%98%D0%B0%20-%20%D0%9D%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D0%BD%D0%B0%20%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D0%B8%D1%98%D0%B0%20%D0%B7%D0%B0%20%D1%81%D0%B0%D1%98%D0%B1%D0%B5%D1%80%20%D0%B1%D0%B5%D0%B7%D0%B1%D0%B5%D0%B4%D0%BD%D0%BE%D1%81%D1%82%202023-2026_%D0%9D%D0%B0%D1%86%D1%80%D1%82_id=45_version=1.pdf

13. Национална стратегија за одбрана и Акциски план за имплементација 2019-2023 година, https://mod.gov.mk/inc/uploads/2021/06/Strategija-za-sajber-odbrana-mk-1-1.pdf

14. Cybercrime Programme Office (C-PROC) of the Council of Europe https://rm.coe.int/octocom-legal-profile-nm-revised-by-nm/16809e5dd6

15. Council of Europe https://www.coe.int/en/web/cybercrime/the-budapest-convention


Насоки
за користење на истражувачките услуги
на Парламентарен институт
Кој ги користи услугите?
-пратениците
-работните тела
-советите
-пратеничките групи
-генералниот секретар
Зошто?
за обезбедување објективни и непристрасни информации заради:
-подобро аргументирање на ставовите;
- подобро запознавање со предлог-законите и другите акти;
-кристализирање на идејата за поднесување предлог-закон;
-учество на јавни настапи, комуникација со граѓани и дипломатски посети
Како?
со поднесување барање за истражувачки работи:
-во писмена форма (на пропишаниот образец, потпишан лично од корисникот)
-во електронска форма (преку системот на е-парламент)
Кому му се поднесува барањето?
на раководителот на Парламентарен институт
(за дополнителни појаснувања во однос на темата и рокот, истражувачот и раководителите се консултираат со корисникот при добивањето на барањето и во текот на изработката на истражувачката работа)
Какви услуги и препорачан минимален рок?
минимум работни дена:
-кратка информација 3
-хронолошки преглед 5
-тематски преглед 5
-компаративен преглед 7
-опширна информација 10
Што содржат истражувачките работи?
истражувачките работи се од информативна природа, политички неутрални и објективни, се фокусираат на факти и не содржат препораки, ниту сугерираат решенија
Што не може да биде побарано?
-правни совети и помош за индивидуални случаи;
-изработка на нацрт-закони или амандмани;
-информации од надлежност на други сектори во Собранието
parl.inst@sobranie.mk
070/409-544
070/352-474
070/320-349
070/320-348
071/305-384