20261061594

РЕГУЛАТОРНА КОМИСИЈА ЗА ЕНЕРГЕТИКА, ВОДНИ УСЛУГИ И УСЛУГИ ЗА УПРАВУВАЊЕ СО КОМУНАЛЕН ОТПАД НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

☐Врз основа на член 65 став (4) од Законот за енергетика* („Службен весник на Република Северна Македонија“ бр.101/2025 и 135/25), а во согласност со Законот за безбедност на мрежни и информациски системи („Службен весник на Република Северна Македонија“ бр.135/2025), Регулаторната комисија за енергетика, водни услуги и услуги за управување со комунален отпад на Република Северна Македонија, на седницата одржана на 11.5.2026 година, донесе

ПРАВИЛА ЗА САЈБЕР-БЕЗБЕДНОСТ НА ОБЈЕКТИТЕ ЗА ПРОИЗВОДСТВО, СКЛАДИРАЊЕ И СИСТЕМИТЕ ЗА ПРЕНОС И ДИСТРИБУЦИЈА НА ЕНЕРГИЈА

ПОГЛАВЈЕ I: ОПШТИ ОДРЕДБИ

Член 1
Предмет на уредување

Со овие Правила поблиску се уредуваат обврските за обезбедување сајбер безбедност, односно техничките и организациските мерки и активности што ги преземаат субјектите од член 65 став (1) на Законот за енергетика, и тоа:

1) определување критична инфраструктура во енергетскиот сектор и приоритети за обезбедување сајбер безбедност;

2) меѓународни стандарди за безбедност на мрежите, информатичка безбедност и сајбер безбедност;

3) основни елементи на методологијата за проценка на ризици од сајбер напади и инциденти и на оперативните планови за превенција и реакција;

4) начин и постапка за проверка на безбедноста на применетите информациски системи;

5) барањата кои треба да ги исполнат новите и постојните уреди поврзани со интернет или кои се користат во мрежите и системите кои применуваат оперативни технологии;

6) мерки и активности за спречување и/или намалување ризици од сајбер напади и инциденти;

7) мерки и активности за спречување и/или намалување ризици од сајбер напади и инциденти предизвикани од и поврзани со домино ефектите;

8) начин, постапка и рокови за доставување известувања за откриени сајбер безбедносни напади и инциденти до Регулаторната комисија за енергетика, водни услугии услуги за управување со комунален отпад на Република Северна Македонија (во натамошниот текст: Регулаторна комисија за енергетика);

9) условите за назначување службеник за сајбер безбедност, неговите овластувања и задачи;

10) основни елементи на програмата за спроведување обуки за вработените за сајбер безбедност и рокови за исполнување на обврските пропишани со овие Правила.

Член 2

Дефиниции

(1) Изразите употребени во овие Правила го имаат значењето утврдено со Законот за енергетика и Законот за безбедност на мрежни и информациски системи.

(2) Одделни изрази употребени во овие Правила го имаат следното значење:

„Сајбер напад" е намерен обид за неовластен пристап, компромитирање, уништување или нарушување на достапноста, интегритетот или доверливоста на мрежи, информациски системи, податоци или услуги;

„Значаен сајбер безбедносен инцидент“ согласно член 3 точка 16 од ЗБМИС е сајбер безбедносен инцидент кој:

а) предизвикал или може да предизвика сериозни нарушувања во функционирањето на услугите или да предизвика финансиски загуби за соодветниот клучен, односно важен субјект;

b) влијаел или може да влијае врз други физички или правни лица со предизвикување значителна материјална или нематеријална штета„

„Сајбер закана" е потенцијална околност, настан или дејствие кое може да нанесе штета на мрежните и информациските системи, на корисниците на тие системи и на другите лица;

„Ранливост" е слабост, чувствителност или дефект на ИКТ производи или ИКТ услуги кој може да биде искористен од сајбер закана;

„Критична инфраструктура" се информатичко комуникациски (ИКТ) средства, системи, објекти, мрежи или нивни делови во енергетскиот сектор со кои се остваруваат витални функции на општеството, а кои се од суштинско значење и прекинот на нивната работа или нивното уништување може да има сериозни последици за безбедноста на граѓаните, економијата или националната безбедност, согласно член 3 точка 29 од ЗБМИС. Определувањето на критична инфраструктура е основ за класификација на субјектот како суштински субјект (ЗБМИС чл.8 ст.1 т.6);

„Критична национална инфраструктура" (КНИ) се средства, системи и мрежи од суштинско значење за државата утврдени согласно закон. КНИ е поширок национален концепт кој ги опфаќа сите сектори, додека критичната инфраструктура од претходната точка е секторски концепт во надлежност на Регулаторната комисија за енергетика;

„Службеник за сајбер безбедност" е лице назначено согласно член 65 став (2) точка 1 од Законот за енергетика кое е одговорно за координација и надзор на активностите за сајбер безбедност кај регулираниот субјект. Овој поим е еквивалентен на поимот „офицер за сајбер безбедност" дефиниран во член 3 точка 35 од Законот за безбедност на мрежни и информациски системи;

„Суштински субјект" е субјект класифициран согласно член 8 став (1) од Законот за безбедност на мрежни и информациски системи, кој: (а) ги исполнува критериумите за голем субјект (чл.8 ст.1 т.1); (б) е утврден како оператор/сопственик на критична инфраструктура, без оглед на големината (чл.8 ст.1 т.6, чл.4 ст.3 т.9); или (в) е утврден како суштински врз основа на националното законодавство или проценка на ризик (чл.8 ст.1 т.7-8);

„Важен субјект" е субјект класифициран согласно член 8 став (2) од Законот за безбедност на мрежни и информациски системи, кој ги исполнува критериумите за среден субјект, а не е класифициран како суштински субјект;

„Орган на управување" е раководен орган на регулираниот субјект кој е одговорен за усвојување на мерките за управување со сајбер безбедносните ризици и надзор над

нивната примена согласно член 31 од Законот за безбедност на мрежни и информациски системи;

„IoT уреди" (Internet of Things) се физички уреди поврзани на интернет или на мрежа, способни да собираат, испраќаат или примаат податоци, вклучувајќи сензори, актуатори, паметни мерачи и слични уреди;

„OT" (Operational Technology) се хардвер и софтвер кои детектираат или предизвикуваат промена преку директно следење и/или контрола на физички уреди, процеси и настани во енергетската инфраструктура;

„Мулти-факторна автентикација" (MFA) е метод на автентикација кој бара два или повеќе независни фактори за верификација на идентитетот;

„Домино ефект" е каскадно ширење на последиците од сајбер инцидент од еден систем или субјект на други поврзани системи или субјекти;

„Ланец на снабдување" се сите добавувачи, подизведувачи, даватели на услуги и други трети страни кои обезбедуваат производи, услуги или компоненти за ИКТ и ОТ системите на регулираниот субјект;

„Криптографија" е примена на математички техники за заштита на доверливоста, интегритетот и автентичноста на податоци преку шифрирање, дигитални потписи, хеш функции и други безбедносни механизми;

„Ризик" е комбинација од веројатноста да настане сајбер инцидент и сериозноста на неговите последици;

„Отпорност" е способност на системите да издржат сајбер напади, да продолжат со критични функции и да се закрепнат брзо по инцидент;

„SIEM" (Security Information and Event Management) е систем за собирање, корелација и анализа на безбедносни настани од повеќе извори во реално време;

„Тестирање преку пенетрација" е симулирање на сајбер напади заради утврдување на отпорноста на системите, апликациите и мрежата.

Член 3

Примена на Правилата

(1) Овие Правила се применуваат на следните субјекти од член 65 став (1) од Законот за енергетика:

- оператори на електропреносниот систем;
- оператори на електродистрибутивниот систем;
- НЕМО (Номиниран оператор на организиран пазар на електрична енергија);
- снабдувачи на електрична енергија;
- производители на електрична енергија кои управуваат со електроцентрали со вкупна инсталирана моќност еднаква или поголема од 200 MW;
- оператори на складишта на електрична енергија со вкупна излезна моќност еднаква или поголема од 50 MW;
- оператори на системот за пренос на гас;
- оператори на системите за дистрибуција на гас;
- оператори на постројки за производство на водород или биогас.

(2) Во натамошниот текст на овие Правила, субјектите од став (1) се нарекуваат „регулирани субјекти".

Член 4

Класификација на регулираните субјекти

(1) Регулираните субјекти се класифицираат како суштински субјекти или важни субјекти согласно критериумите утврдени во член 8 од Законот за безбедност на мрежни и информациски системи.

(2) Класификацијата се врши врз основа на:

а) големината на субјектот — голем или среден субјект, согласно Законот за трговски друштва (ЗБМИС чл.3 точки 4 и 52);

б) статусот на оператор/сопственик на критична инфраструктура утврден согласно член 5 од овие Правила (ЗБМИС чл.8 ст.1 т.6 и чл.4 ст.3 т.9); и

в) проценка на ризик извршена од Регулаторната комисија за енергетика (ЗБМИС чл.8 ст.1 т.8 и чл.8 ст.3).

(3) Како суштински субјекти се класифицираат регулираните субјекти кои:

а) ги исполнуваат критериумите за голем субјект согласно член 8 став (1) точка 1 од ЗБМИС;

б) се утврдени како оператори/сопственици на критична инфраструктура согласно член 5 од овие Правила и член 8 став (1) точка 6 од ЗБМИС, без оглед на нивната големина; или

в) се утврдени како суштински субјекти врз основа на националното законодавство или проценка на ризик согласно член 8 став (1) точки 7 и 8 од ЗБМИС.

(4) Како важни субјекти се класифицираат регулираните субјекти кои ги исполнуваат критериумите за среден субјект согласно член 8 став (2) точка 1 од ЗБМИС, а не се класифицирани како суштински субјекти согласно став (3) на овој член.

(5) Регулираните субјекти кои не ги исполнуваат критериумите за среден или голем субјект, но се утврдени како оператори на критична инфраструктура согласно член 5 од овие Правила, се класифицираат како суштински субјекти согласно член 4 став (3) точка 9 и член 8 став (1) точка 6 од ЗБМИС.

(6) Регулираните субјекти од член 3 кои не ги исполнуваат критериумите за среден или голем субјект и не се утврдени како оператори на критична инфраструктура, ги исполнуваат обврските утврдени со Законот за енергетика член 65 став (1) и овие Правила пропорционално на нивната големина и ризичен профил, согласно член 6 став (7) од ЗБМИС.

(7) Регулаторната комисија за енергетика, како надлежен орган за енергетскиот сектор согласно член 11 став (2) и член 17 став (1) од ЗБМИС, го подготвува списокот на суштински и важни субјекти во енергетскиот сектор и го доставува до Министерството за дигитална трансформација, согласно член 8 став (4) од ЗБМИС.

(8) Регулираните субјекти се должни во рок од два месеци од денот на отпочнување на примената на ЗБМИС, а за новоосновани субјекти од денот на регистрација, да се регистрираат кај Регулаторната комисија за енергетика доставувајќи ги податоците од член 8 став (5) од ЗБМИС: назив, адреса, контакт информации, IP адресни опсези и по потреба секторот и подсекторот. По барање од Регулаторната комисија за енергетика за дополнителни податоци заради проценка на ризик, регулираниот субјект ги доставува податоците на потребното ниво на детали во рок од 20 дена од денот на приемот на барањето.

(9) Обврските утврдени со овие Правила се пропорционални на класификацијата на субјектот. Суштинските субјекти ги исполнуваат сите обврски во целост. Важните субјекти ги исполнуваат обврските пропорционално на нивната големина и ризичниот профил.

(10) Регулаторната комисија за енергетика може да изврши прекласификација доколку настанат промени во големината, статусот на критична инфраструктура или ризичниот профил на субјектот.

(11) Регулираните субјекти од член 3 на овие Правила се во исклучива надлежност на Регулаторната комисија за енергетика како надлежен орган согласно член 11 став (2) од ЗБМИС. Регулаторната комисија за енергетика и Агенцијата за електронски комуникации склучуваат меморандум за соработка за усогласување на евиденциите, размена на информации и координирани вежби.

(12) Класификацијата на регулираните субјекти задолжително се преиспитува и ажурира најмалку еднаш во две години, како и при значајни промени во големината, статусот на критична инфраструктура или ризичниот профил.

ПОГЛАВЈЕ II: ОРГАНИЗАЦИСКА СТРУКТУРА ЗА САЈБЕР БЕЗБЕДНОСТ

Член 5
Критична инфраструктура и приоритети

(1) Регулираните субјекти ги идентификуваат и до Регулаторната комисија за енергетика го предлагаат определувањето на објекти, системи, мрежи и опрема кои претставуваат критична инфраструктура.

(2) Регулаторната комисија за енергетика донесува одлука за определување на критична инфраструктура врз основа на следните критериуми: влијание врз сигурноста на снабдување; влијание врз други критични инфраструктури; економско влијание; влијание врз јавната и националната безбедност; меѓузависности и ризик од домино ефекти; можност за компензација.

(3) Регулаторната комисија за енергетика утврдува приоритет во обезбедувањето на сајбер безбедност на критичната инфраструктура согласно член 65 став (4) точка 1 од Законот за енергетика.

(4) Определувањето на критична инфраструктура согласно став (2) од овој член е основ за класификација на субјектот како суштински субјект согласно член 4 став (3) точка б) од овие Правила и член 8 став (1) точка 6 од ЗБМИС, без оглед на неговата големина. Субјектите утврдени како оператори/сопственици на критична инфраструктура се опфатени со ЗБМИС согласно член 4 став (3) точка 9 од тој закон.

(5) Регулаторната комисија за енергетика доставува предлог до надлежниот орган за определување на критична национална инфраструктура (КНИ) во енергетскиот сектор. Определувањето на КНИ е национален процес кој не влијае на класификацијата по ЗБМИС, но утврдува дополнителен приоритет.

(6) Регулираните субјекти ја категоризираат критичната инфраструктура и КНИ со градација во приоритетот, динамиката на примена на мерки и сертифицирање.

(7) Регулираните субјекти кои вршат јавна услуга ги вклучуваат трошоците за мерките од овој член во пресметката на тарифата согласно прописите за енергетика.

Член 6
Службеник за сајбер безбедност

(1) Регулираните субјекти се должни да назначат службеник за сајбер безбедност согласно член 65 став (2) точка 1 од Законот за енергетика. Одлуката за назначување се доставува до Регулаторната комисија за енергетика во рок од 30 дена, од денот на усвојување на Правилата.

Суштинските субјекти согласно расположливите ресурси можат да назначат и заменик на службеникот за сајбер безбедност и/или тим за сајбер-безбедност и дефинираат детална систематизација со опис на работните места и задачи.

(2) За службеник за сајбер безбедност се назначува лице кое:

а) со правосилна судска пресуда нема изречено казна или прекршочна санкција забрана за вршење на професија;

б) има завршено високо образование во областа на информатичките технологии, електротехниката, телекомуникациите или правото со специјализација во сајбер безбедност;

в) има познавања за SCADA, DCS, ICS системи, ISO 27001, ISO 27019 и IEC 62443; г) има најмалку 3 години работно искуство во управување со ИТ или ОТ и во нивната сајбер безбедност.

(3) Службеникот може да биде лице кое е CISO или друго раководно лице, доколку ги исполнува условите од став (2).

(4) Службеникот може да ги извршува задачите со користење услуги од надлежниот CSIRT, Националниот CSIRT и надворешни експерти за сајбер безбедност.

(5) Задачите и овластувањата на службеникот за сајбер безбедност вклучуваат: спроведување и надзор на примената на овие Правила и други прописи; следење и примена на меѓународни стандарди; изработка на сајбер безбедносна програма; откривање на слабости и ризици; дефинирање сценарија и проценка на ризици; следење на ранливости; иницирање и надзор на ажурирањето на хардвер и софтвер; координација при инциденти; комуникација со раководство, РКЕ и CSIRT.

(6) Службеникот е овластен да пристапува до сите ИКТ и ОТ системи, да бара информации од сите организациски единици, да дава налози за итни мерки и директно да ја известува управата.

(7) Органот на управување на регулираниот субјект, согласно член 31 од Законот за безбедност на мрежни и информациски системи, е одговорен за: а) усвојување на мерките за управување со сајбер безбедносните ризици; б) надзор над имплементацијата на мерките; в) обезбедување соодветни ресурси; г) учество во обука за сајбер безбедност.

(8) При престанок на функцијата на службеникот, регулираниот субјект назначува нов службеник во рок од 30 дена.

(9) Офицерите за сајбер безбедност имаат право и обврска да поминуваат континуиран професионален развој за да обезбедат ефективно извршување на своите работни задачи. Иако специфичните професионални сертификати не се експлицитно задолжени, силно се препорачува обезбедување на меѓународно признати професионални сертификати за офицерите за сајбер безбедност, согласно препораките на Министерството за дигитална трансформација.

Член 7

Тим за сајбер безбедност и безбедност на човечки ресурси

(1) Суштинските субјекти согласно потребите и ресурсите формираат тим за сајбер безбедност составен од стручни лица за сајбер безбедност, со улога за поддршка и операционализација на активностите пропишани со овие правила и под надзор над одредениот Службеник за сајбер-безбедност. Суштинските субјекти задолжително назначуваат Службеник за сајбер безбедност и воспоставуваат внатрешни основни човечки ресурси за сајбер безбедност, но можат да ангажираат надворешни експерти за специјализирани функции (пенетрациско тестирање, SOC мониторинг, форензика). Целосно аутсорсирање не е дозволено за суштинските субјекти. Важните субјекти може да ангажираат надворешни експерти за извршување на оваа функција.

(2) Тимот за сајбер безбедност врши: континуирано следење на мрежните и информациските системи; детекција на сајбер закани и аномалии; анализа и одговор на инциденти; управување со ранливости; координација со надлежниот CSIRT и Регулаторната комисија за енергетика; спроведување безбедносни тестирања.

(3) Регулираните субјекти воспоставуваат политики за безбедност на човечки ресурси согласно член 32 став (3) точка 9 од ЗБМИС, кои вклучуваат: проверка на безбедноста на вработените (background check); договори за доверливост; дефинирани улоги и одговорности за сајбер безбедност; процедури за доделување и одземање на пристапни права; процедури при заминување на вработени (offboarding).

(4) Пристапните права се доделуваат според принципот на најмала привилегија (least privilege) и се прегледуваат периодично согласно проценатa на ризик, најмалку еднаш годишно.

ПОГЛАВЈЕ III: УПРАВУВАЊЕ СО РИЗИЦИ И СТАНДАРДИ

Член 8
Проценка на ризици, регистар на ризици и справување со ризици

(1) Регулираните субјекти воспоставуваат систем за управување со сајбер безбедносни ризици согласно член 32 став (3) точка 1 од ЗБМИС. Проценката на ризици се врши согласно ISO/IEC 27005 и опфаќа: идентификација на критични средства, закани и ранливости; проценка на веројатност и влијание; определување ниво на ризик; дефинирање мерки за третман. Деталната методологија е дадена во Прилог 5.

(2) Органот на управување на регулираниот субјект ја усвојува годишната проценка на ризици согласно член 31 став (1) од ЗБМИС.

(3) Проценката на ризици се врши: при иницијално воспоставување на системот; најмалку еднаш годишно; по значајни промени во мрежните и информациските системи; по секој значаен сајбер безбедносен инцидент.

(4) Регулираните субјекти водат Регистар на ризици кој содржи: идентификатор; опис; категорија; засегнати средства; закани; ранливости; веројатност; влијание; ниво на ризик; контроли; остаточен ризик; стратегија за третман; одговорно лице; рокови; статус. Регистарот се ажурира најмалку квартално.

(5) Регулираните субјекти донесуваат План за справување со ризици кој содржи приоритизирани ризици, стратегии за третман (прифаќање, ублажување, пренесување или избегнување), мерки, одговорни лица, рокови и индикатори за успешност.

(6) Извештајот за проценка на ризици со информација за најмалку критични и високи ризици се доставува до Регулаторната комисија за енергетика најдоцна до 31 март за претходната година.

Член 9
Сертификација според меѓународни стандарди и модел за сајбер безбедносна подготвеност

(1) Регулираните субјекти имплементираат систем за управување со безбедноста на информациите (ISMS) во согласност со ISO/IEC 27001:2022. Суштинските субјекти се должни да се сертифицираат во рок од 18 месеци од влегувањето во сила на овие Правила. Важните субјекти имплементираат ISMS и поднесуваат годишна потврда за усогласеност до Регулаторната комисија за енергетика, како дел од Годишен извештај. Сертификацијата се обновува на секои три години со годишни надзорни аудити. Годишните надзорни аудити се вршат од страна на независна сертификациона организација акредитирана за ISO/IEC 27001:2022; извештајот од надзорниот аудит се доставува до Регулаторната

комисија за енергетика како составен дел на годишниот извештај за сајбер безбедност (член 22 став 3), а за важните субјекти кога Регулаторната комисија за енергетика тоа го бара по проценка на ризик или по значаен инцидент.

(2) За субјекти со критична инфраструктура се препорачува и примена на ISO/IEC 27019:2017 (енергетски сектор) и IEC 62443 (индустриски системи).

(5) Регулаторната комисија за енергетика ги зема предвид трошоците за сертификација при определување на тарифите за субјекти со обврска за јавна услуга.

(6) Регулираните субјекти при набавка на ИКТ производи и услуги може да бараат сертификати согласно член 35 од ЗБМИС.

Член 10

Домино ефекти и меѓузависности

(1) Регулираните субјекти спроведуваат проценка на потенцијални домино ефекти и меѓузависности со други енергетски субјекти, критични инфраструктури и сектори, согласно член 65 став (4) точка 7 од Законот за енергетика.

(2) Проценката опфаќа: идентификација на технички, оперативни и географски меѓузависности; анализа на каскадни ефекти помеѓу поврзани мрежи и системи; идентификација на точки на единечен прекин (Single Points of Failure); дефинирање мерки за ограничување на каскадни ефекти.

(3) Регулираните субјекти со значајни меѓузависности воспоставуваат договори за размена на информации, координирани процедури за одговор на инциденти и заеднички вежби.

(4) Проценката на домино ефекти се доставува до Регулаторната комисија за енергетика најдоцна до 31 март како дел од годишниот извештај за сајбер безбедност, и се ажурира најмалку еднаш годишно.

(5) Регулаторната комисија за енергетика може да иницира координирани заеднички проценки кога значајни меѓузависности се идентификувани кај повеќе субјекти.

ПОГЛАВЈЕ IV: ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Член 11

Технички мерки за сајбер безбедност

(1) Регулираните субјекти имплементираат технички мерки за сајбер безбедност согласно член 32 став (3) од ЗБМИС и барањата утврдени во Прилог 1 на овие Правила, и тоа за следните области:

а) мрежна безбедност и сегментација (вклучувајќи ИТ/ОТ сепарација, DMZ, firewall, IDS/IPS);

б) контрола на пристап и управување со идентитети (согласно чл.32 ст.3 т.9 од ЗБМИС);

в) мулти-факторна автентикација за далечински пристап, привилегирани сметки и критични системи (согласно чл.32 ст.3 т.10 од ЗБМИС);

г) управување со ранливости и закрпи (согласно чл.32 ст.3 т.5 од ЗБМИС);

д) системи за континуирано следење и откривање (SIEM, SOC, EDR);

ѓ) логирање, чување и анализа на безбедносни настани;

е) криптографија и шифрирање (согласно чл.32 ст.3 т.8 од ЗБМИС);

ж) безбедност на IoT уреди и ОТ системи (согласно чл.65 ст.4 т.5 од ЗЕ);

з) безбедност при набавка, развој и одржување на мрежни и информациски системи (согласно чл.32 ст.3 т.5 од ЗБМИС);

s) физичка безбедност на ИКТ и ОТ системи.

(2) Мерките се избираат врз основа на проценката на ризик и се пропорционални на класификацијата на субјектот.

(3) Регулираните субјекти вршат внатрешно и надворешно пенетрациско тестирање најмалку еднаш годишно. Информација со сумарни наоди од тестирање се доставува до Регулаторната комисија за енергетика во рок од 30 дена од завршувањето на тестирањето и се вклучува во годишниот извештај за сајбер безбедност. Целосниот извештај треба е достапен на увид по барање од Регулаторната комисија за енергетика. Во опфатот на тестирањето задолжително се вклучува идентификуваната критична инфраструктура. Тестирањето треба да е спроведено од страна на надворешни ангажирани стручни лица. Тестирањето на ИТ средината се изведува задолжително еднаш годишно. За ОТ се применуваат не-нарушувачки техники; активни тестови само за време на планирани термини за одржување или каде постои редундантност, согласно можностите.

(4) Регулираните субјекти водат евиденција за имплементираните мерки, нивната ефикасност, надградба или замена.

(5) Регулираните субјекти мора да се усогласат и со законодавството за заштита на лични податоци при имплементација на сајбер безбедносните мерки, особено субјектите кои обработуваат податоци за потрошувачи.

Член 12

Организациски мерки за сајбер безбедност

(1) Регулираните субјекти имплементираат организациски мерки за сајбер безбедност согласно барањата утврдени во Прилог 2 на овие Правила, и тоа за следните области:

а) политики и процедури за сајбер безбедност;

б) управување со средства (asset management) — инвентар на ИКТ и ОТ средства;

в) управување со промени (change management);

г) класификација на податоци и информации;

д) документација и евиденција.

(2) Организациските мерки се донесуваат и спроведуваат координирано со техничките мерки од член 11.

(3) Политиките и процедурите се прегледуваат и ажурираат најмалку еднаш годишно.

(4) Регулираните субјекти воспоставуваат политики и постапки за проценка на ефикасноста на мерките за управување со сајбер безбедносните ризици согласно член 32 став (3) точка 6 од ЗБМИС.

Член 13

Безбедност на ланецот на снабдување

(1) Регулираните субјекти управуваат со безбедносни ризици во ланецот на снабдување согласно член 32 став (3) точка 4 од ЗБМИС и барањата утврдени во Прилог 3 на овие Правила.

(2) При определувањето на мерките за безбедност на ланецот на снабдување, регулираните субјекти ја имаат предвид ранливоста што е специфична за секој непосреден добавувач и давател на услуги, квалитетот на производите и нивната сајбер безбедносна пракса, вклучувајќи ги и нивните безбедни развојни постапки, согласно член 32 став (4) од ЗБМИС.

(3) Пред набавка на ИКТ или ОТ производи или услуги, регулираните субјекти спроведуваат проценка на безбедноста на добавувачот, врз основа на имплементираните стандарди за безбедност на добавувачот.

(4) Договорите со добавувачи содржат безбедносни барања: известување за ранливости; обезбедување безбедносни ажурирања; право на ревизија; политика за крај на животен век; инцидентно известување.

(5) Критичните добавувачи (добавувачи на опрема која е дел од идентификуваната критична инфраструктура) се преоценуваат најмалку еднаш годишно.

ПОГЛАВЈЕ V: УПРАВУВАЊЕ СО ИНЦИДЕНТИ

Член 14
Откривање и класификација на инциденти

(1) Регулираните субјекти воспоставуваат процеси за откривање, класификација и приоритизација на сајбер безбедносни инциденти согласно член 32 став (3) точка 2 од ЗБМИС, матрицата во Прилог 4 и методологијата во Прилог 7.

(2) Инцидентите се класифицираат на: а) значајни сајбер безбедносни инциденти, согласно Член 2 од овие Правила и б) обични сајбер безбедносни инциденти, сите останати инциденти кои не ги исполнуваат критериумите за значајност.

(3) Регулаторната комисија за енергетика, како надлежен орган согласно член 11 од ЗБМИС, донесува методологија за поблиските критериуми и прагови за определување на обични и значајни сајбер безбедносни инциденти во енергетскиот сектор, по претходна согласност на Министерството, а која се ажурира најмалку еднаш годишно, најдоцна до 28 февруари за тековната година, согласно член 33 став (12) од ЗБМИС. Предлог методологијата е содржана во Прилог 7 кој е составен дел на овие Правила.

(4) Регулираните субјекти воспоставуваат евиденција на инциденти која се чува најмалку 5 години за значајните инциденти, и најмалку 2 (две) за останатите инциденти.

(5) За значајни инциденти регулираниот субјект задолжително спроведува анализа на основната причина (Root Cause Analysis) и пост инцидентна анализа.

(6) При откривање на значаен инцидент, регулираниот субјект задолжително обезбедува зачувување на дигитални докази со примена на принципите на интегритет, автентичност, следливост и синџир на старателство (chain of custody): хеширање на докази со SHA-256 или посилен алгоритам, временски печати, идентитет на лицето кое ја извршило активноста, и заштита на логови, артефакти и нивните копии од измена или бришење најмалку 12 месеци.

Член 15
Известување за значајни сајбер безбедносни инциденти

(1) Регулираните субјекти се должни веднаш, а најдоцна во рок од три часа од моментот на дознавањето за настанување на значаен сајбер безбедносен инцидент и/или значајна сајбер закана, да го известат надлежниот тим за одговор на компјутерски инциденти и Регулаторната комисија за енергетика, доставувајќи ги сите информации со кои ќе се овозможи утврдување на прекуграничното влијание на инцидентот, согласно член 33 став (1) од ЗБМИС.

(2) Надлежен тим за одговор на компјутерски инциденти (CSIRT) за енергетскиот сектор е MKD-CIRT, согласно член 17 став (4) од ЗБМИС. Со посебен закон или преку

јавно-приватно партнерство може да се воспостави секторски CSIRT за енергетиката, согласно член 17 став (3) од ЗБМИС.

(3) Доколку е можно, регулираните субјекти се должни, веднаш, а најдоцна наредниот работен ден од моментот на дознавањето за сериозна сајбер закана, да ги известат засегнатите корисници на нивните услуги за сите мерки или правни средства кои тие можат да ги преземат како одговор на заканата, согласно член 33 став (2) од ЗБМИС.

(4) Регулираните субјекти за значајни сајбер безбедносни инциденти известуваат во четиристепена структура согласно член 33 став (3) од ЗБМИС и шаблоните во Прилог 4:

ФАЗА 1 — ИНИЦИЈАЛНО ИЗВЕСТУВАЊЕ (3 часа од дознавањето): идентификација на субјект; датум и време на откривање; тип на инцидент или закана; засегнати услуги; прелиминарна проценка на влијание; информации за можно прекугранично влијание.

ФАЗА 2 — РАНО ПРЕДУПРЕДУВАЊЕ (24 часа од дознавањето): ажурирани информации од Фаза 1; проценка дали инцидентот е предизвикан од незаконско или злонамерно дејствување; проценка за можно прекугранично влијание, согласно член 33 став (3) точка 1 од ЗБМИС.

ФАЗА 3 — ДЕТАЛНО ИЗВЕСТУВАЊЕ (72 часа од дознавањето): ажурирани информации од Фаза 2; почетна проценка на сериозноста и влијанието ; показатели за загрозеност (IOCs); детален опис и временска рамка; вектор на напад, согласно член 33 став (3) точка 2 од ЗБМИС.

ФАЗА 4 — ЗАВРШНО ИЗВЕСТУВАЊЕ (1 месец по Фаза 3): детален опис на инцидентот вклучувајќи ја неговата сериозност и влијание; типот на закана или главната причина што го предизвикала инцидентот; мерки за ублажување што се примениле и се применуваат; прекугранично влијание доколку е соодветно, согласно член 33 став (3) точка 4 од ЗБМИС.

(4) На барање од надлежниот тим за одговор на компјутерски инциденти, регулираните субјекти доставуваат привремени известувања за релевантните ажурирања на статусот, согласно член 33 став (3) точка 3 од ЗБМИС. Регулираниот субјект за истото без одложување известува до Регулаторната комисија за енергетика.

(5) Доколку значајниот инцидент е во тек во моментот на поднесувањето на завршното известување, субјектот доставува извештај за напредок и завршно известување во рок од еден месец од решавањето на инцидентот, согласно член 33 став (3) точка 5 од ЗБМИС.

(6) Регулаторната комисија за енергетика, како примател на известувањето, е должна без непотребно одлагање, а не подоцна од два часа од моментот на прием, да го проследи истото до надлежниот тим за одговор на компјутерски инциденти, согласно член 33 став (1) од ЗБМИС.

(7) Регулаторната комисија за енергетика и Надлежниот CSIRT се должни да воспостават редундантни канали за комуникација, размена на информации и пријава на инциденти со Регулираните субјекти. Во случај на прекин и недостапност на основниот канал за комуникација, Регулираните субјекти ќе користат (out-of-band) канал за комуникација со Регулаторната комисија за енергетика и CSIRT при инциденти

(8) Квартални извештаи за инциденти се доставуваат до Регулаторната комисија за енергетика до петтиот ден по завршувањето на кварталот.

Член 16

Одговор на инциденти и закрепнување

(1) Регулираните субјекти воспоставуваат План за одговор на инциденти кој содржи: тим за одговор; фази на одговор (подготовка, детекција, ограничување, елиминација,

закрепнување, постинцидентна анализа); процедури за ескалација; комуникациски процедури. Планот за одговор на инциденти задолжително се усогласува со националните планови за одговор на инциденти и процедурите на надлежниот CSIRT (MKD-CIRT).

(2) Суштинските субјекти обезбедуваат достапност на тимот за одговор.

(3) Планот се тестира преку симулации најмалку еднаш годишно и се ажурира по секој значаен инцидент.

Член 17

Координација и споделување информации

(1) Регулаторната комисија за енергетика го координира споделувањето на информации за сајбер закани, ранливости и инциденти помеѓу регулираните субјекти, согласно член 65 став (2) точка 4 од Законот за енергетика и член 37 од ЗБМИС.

(2) Информациите за споделување вклучуваат: показатели за загрозеност (IOCs); нови закани и ранливости; тактики, техники и процедури на напаѓачи (TTPs). Размената се врши согласно протоколот Traffic Light Protocol (TLP) верзија 2.0 или преку MISP инфраструктура, или еквивалентна доверлива платформа за размена на индикатори на загрозеност.

(3) Доколку инцидент може да влијае на други субјекти поради меѓузависности, засегнатите субјекти итно се известуваат од страна на Регулаторна комисија за енергетика.

(5) Регулаторната комисија за енергетика остварува соработка со MKD-CIRT и Министерството за дигитална трансформација за размена на информации за закани, ранливости и инциденти во енергетскиот сектор.

(6) Регулираните субјекти можат доброволно да известуваат за инциденти, сајбер закани и ранливости согласно член 38 од ЗБМИС.

ПОГЛАВЈЕ VI: ДЕЛОВЕН КОНТИНУИТЕТ И УПРАВУВАЊЕ СО КРИЗИ

Член 18

Деловен континуитет, закрепнување и резервни копии

(1) Регулираните субјекти изготвуваат и одржуваат планови согласно член 32 став (3) точка 3 од ЗБМИС:

а) План за деловен континуитет (BCP) — анализа на влијание, стратегии за континуитет, процедури за активирање;

б) План за закрепнување по катастрофален испад (DRP) — стратегии за закрепнување, детални процедури за опоравување на системи;

в) Политика за резервни копии — правило 3-2-1, шифрирање, непроменливи и физички изолирани копии. Правило 3-2-1 предвидува три копии на податоците, на најмалку два различни типа медиуми, со најмалку една копија на оддалечена или физички изолирана локација. Фреквенцијата за критични OT конфигурации се определува врз основа на проценка на ризик.

(2) Плановите се однесуваат на критичните системи и услуги согласно категоризацијата на регулираниот субјект, и содржат дефинирани целни времиња за закрепнување (RTO) и целни точки за закрепнување (RPO) за критичните системи и услуги.

(3) Тестирање: Регулираните субјекти се должни да спроведуваат вежби за BCP најмалку еднаш годишно, како и најмалку квартално спроведување на тестови за обновување на резервни копии за критични системи. Суштинските субјекти се должни да спроведуваат целосни DR вежби најмалку еднаш годишно.

(4) Плановите се ажурираат најмалку еднаш годишно и се доставуваат до Регулаторната комисија за енергетика најдоцна до 31 март, заедно со годишниот извештај за сајбер безбедност. Иницијалните планови се доставуваат во рокот утврден во Фаза 2 од член 24.

(5) При сајбер напад, регулираните субјекти неделно го пријавуваат степенот на оперативност до целосно закрепнување.

Член 19

Управување со сајбер кризи

(1) Регулираните субјекти изготвуваат План за управување со сајбер кризи за сериозни инциденти кои влијаат на јавната безбедност, сигурноста на снабдување или критичната национална инфраструктура, согласно член 32 став (3) точка 3 од ЗБМИС. Суштинските субјекти изготвуваат целосен план за управување со сајбер кризи; важните субјекти изготвуваат најмалку процедури за кризна ескалација поврзани со националната рамка согласно ЗБМИС.

(2) Планот содржи: критериуми за прогласување криза; тим за управување со кризи; процедури за внатрешна и надворешна комуникација (вклучувајќи медиуми, РКЕ, CSIRT, државни органи); процедури за ескалација на национално ниво; критериуми за завршување на кризата.

(3) Доколку за спречување или за решавање на значаен сајбер безбедносен инцидент е потребно да се извести јавноста, Регулаторната комисија за енергетика може, по консултација со засегнатиот субјект, да побара јавно известување согласно член 33 став (10) од ЗБМИС.

(4) Тестирање: тематски вежби на маса за управување со кризи најмалку еднаш годишно; функционални вежби најмалку еднаш на две години за суштинските субјекти.

(5) Извршно резиме од Планот за управување со кризи се доставува до Регулаторната комисија за енергетика најдоцна до 31 март, заедно со годишниот извештај за сајбер безбедност. Извршното резиме од Иницијалниот план се доставува во рокот утврден во Фаза 2 од член 24.

ПОГЛАВЈЕ VII: ОБУКА И ПОДИГАЊЕ НА СВЕСТ

Член 20

Програма за обука

(1) Регулираните субјекти изготвуваат и применуваат програма за обука согласно член 65 став (2) точка 5 од Законот за енергетика и член 32 став (3) точка 7 од ЗБМИС, која содржи: основна обука за сите вработени; напредна обука за ИТ/ОТ персонал; специјализирана обука за тимот за сајбер безбедност; обука за раководство.

(2) Органот на управување на регулираниот субјект мора да учествува во обука за сајбер безбедност согласно член 31 став (2) од ЗБМИС.

(3) Фреквенција: иницијална обука за нови вработени во рок од 30 дена; годишна обука за сите вработени; целни обуки по значајни инциденти.

(4) Годишен извештај за спроведени обуки се доставува до Регулаторната комисија за енергетика најдоцна до 31 март, како дел од годишниот извештај за сајбер безбедност.

Член 21

Симулации, вежби и сајбер хигиена

(1) Регулираните субјекти спроведуваат активности за подигање на свест и основни практики за сајбер хигиена согласно член 32 став (3) точка 7 од ЗБМИС. Активностите вклучуваат: (а) обука и подигање на свеста за принципите на сајбер хигиена и (б) имплементација и спроведување на основни практики како организациски барања (политики за лозинки, ажурирања, безбедни конфигурации, управување со уреди).

(2) Регулираните субјекти задолжително спроведуваат phishing симулации; суштинските најмалку квартално, важните субјекти најмалку полугодишно. суштинските субјекти спроведуваат: phishing симулации (квартално); тематски вежби на маса (годишно);

(3) Регулираните субјекти задолжително спроведуваат тематски вежби на маса, најмалку еднаш годишно. Вежбите опфаќаат најмалку: (а) процедури за одговор на инциденти; (б) активирање на план за обновување од катастрофа; (в) кризна комуникација и ескалација. Учесници: службеник, тим за сајбер безбедност, претставници на управата и клучен оперативен персонал.

(4) По секоја тематска вежба на маса се изготвува извештај со резултати и препораки. Годишен извештај за симулации и вежби се доставува до Регулаторната комисија за енергетика најдоцна до 31 март, како дел од годишниот извештај за сајбер безбедност.

ПОГЛАВЈЕ VIII: НАДЗОР И ИЗВЕСТУВАЊЕ

Член 22
Годишни планови, извештаи и надзор

(1) Регулираните субјекти изготвуваат годишен план за сајбер безбедност и го доставуваат до Регулаторната комисија за енергетика најдоцна до 31 јануари за тековната година, согласно член 65 став (3) од Законот за енергетика.

(2) Годишниот план за сајбер безбедност задолжително ги содржи следните елементи:

а) стратешки цели за сајбер безбедност за тековната година;

б) преглед на идентификувани ризици и приоритети;

в) планирани технички и организациски мерки;

г) план за обуки и симулации;

д) буџетски рамки за сајбер безбедност;

ѓ) временска рамка за имплементација;

е) план за сертификација и усогласување;

ж) план за тестирање на деловен континуитет.

(3) Регулираните субјекти изготвуваат годишен извештај за сајбер безбедност кој го доставуваат до регулаторната комисија за енергетика најдоцна до 31 март, кој содржи:

а) статус на усогласеност; годишна проценка на ризици (усвоена од органот на управување согласно ЗБМИС чл.31 ст.1);

б) статус на сертификација;

в) резиме на инциденти;

г) анализа на домино ефекти;

д) статус на обуки и симулации;

ѓ) проценка на ефикасност на мерки согласно ЗБМИС чл.32 ст.3 т.6.

(4) Регулаторната комисија за енергетика спроведува проактивен надзор над суштинските субјекти и ex-post надзор над важните субјекти, согласно членови 49 до 52 од ЗБМИС.

(5) Проверките опфаќаат: документација; интервјуа; физички преглед; технички контроли; статус на претходни препораки.

(6) Регулаторната комисија за енергетика го изготвува годишниот план за надзор најдоцна до 31 декември за наредната година, согласно член 273 од Законот за енергетика.

(7) Консолидиран календар на известувања и извештаи:

а) 31 јануари — годишен план за сајбер безбедност (став 1);

б) 31 март — годишен извештај за сајбер безбедност (став 3), кој вклучува: извештај за проценка на ризици (чл. 8 ст. 6); проценка на домино ефекти (чл. 10 ст. 4); информација со сумарни наоди од тестирање (чл. 11 ст. 3); ажурирани планови за деловен континуитет и закрепнување (чл. 18 ст. 4); план за управување со кризи (чл. 19 ст. 5); извештај за обуки (чл. 20 ст. 4); извештај за симулации и вежби (чл. 21 ст. 4); проценка на ефикасност на мерки (чл. 23 ст. 5);

в) 5-ти ден по кварталот — квартален извештај за инциденти (чл. 15 ст. 7);

г) 3 часа / 24 часа / 72 часа / 1 месец — фазно известување за значајни инциденти (чл. 15 ст. 3);

д) неделно — извештај за оперативност при сајбер напад до целосно закрепнување (чл. 18 ст. 5);

ѓ) во рок од 30 дена — информација со сумарни наоди од тестирање по завршување на тестирањето (чл. 11 ст. 3);

е) во рок од 30 дена — одлука за назначување/замена на службеник за сајбер безбедност (чл. 6 ст. 1).

Член 23

Санкции и оценка на ефикасност на мерки

(1) За неисполнување на обврските од овие Правила, Регулаторната комисија за енергетика може да преземе мерки согласно Законот за енергетика и Законот за безбедност на мрежни и информациски системи.

(2) Регулираните субјекти воспоставуваат политики и постапки за проценка на ефикасноста на мерките за управување со сајбер безбедносните ризици согласно член 32 став (3) точка 6 од ЗБМИС, користејќи соодветни клучни показатели на перформансите.

(3) Извештајот за проценка на ефикасност се вклучува во годишниот извештај.

ПОГЛАВЈЕ IX: ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 24

Фазна имплементација и рокови за усогласување

(1) Имплементацијата на обврските од овие Правила се спроведува фазно:

Фаза 1 (6 месеци од влегувањето во сила): назначување службеник за сајбер безбедност; формирање тим за сајбер безбедност (суштински субјекти); иницијален попис на средства (хардвер, софтвер, мрежни средства, ОТ системи) согласно Прилог 2, Дел 2.1.; иницијална проценка на ризици; основни политики за сајбер безбедност; воспоставување процес за управување со инциденти; MFA за далечински пристап.

Фаза 2 (12 месеци од влегувањето во сила): сите регулирани субјекти имаат обврска за целосна проценка на ризици и водење на регистар; планови за деловен континуитет и закрепнување; програма за обука; прв годишен извештај; мрежна сегментација ИТ/ОТ; систем за резервни копии.

Фаза 3 (18 месеци од влегувањето во сила): суштинските субјекти — ISO 27001 сертификација; SIEM; целосни технички и организациски мерки; проценка на домино ефекти и безбедност на ланецот на снабдување.

Фаза 4 (24 месеци од влегувањето во сила): важните субјекти — целосно усогласување со сите обврски од овие Правила.

(2) Доколку регулираниот субјект не може да се усогласи во утврдениот рок, може да поднесе образложено барање за продолжување најдоцна 60 дена пред истекот на рокот, со наведени предложени привремени компензирачки мерки.

(3) По истекот на роковите од став (1), регулираните субјекти континуирано ги одржуваат и подобруваат мерките за сајбер безбедност.

Член 25

Престанок на важење и влегување во сила

Со денот на влегувањето во сила на овие Правила, престануваат да важат Правилата за сајбер безбедност бр.01-1324/1 донесени на седницата одржана на 08.06.2023 година.

Овие Правила влегуваат во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Регулаторна комисија за енергетика, водни услуги и услуги за управување со комунален отпад на Република Северна Македонија
Претседател,
Ацо Ристов, с.р.

Бр. 01-737/1
11 мај 2026 година
Скопје

ПРИЛОГ 1

ТЕХНИЧКИ МЕРКИ ЗА САЈБЕР БЕЗБЕДНОСТ

Согласно член 11 од овие Правила, следува листа на Технички мерки за сајбер безбедност кои регулираните субјекти се должни да ги имплементираат, согласно класификација.

1. МРЕЖНА БЕЗБЕДНОСТ И СЕГМЕНТАЦИЈА

1.1 Мрежна сегментација:

а) физичка или логичка сегментација на мрежите во безбедносни зони (корпоративна ИТ мрежа, DMZ, ОТ мрежа, IoT мрежа);

б) строга сепарација помеѓу ИТ и ОТ мрежи;

в) изолација на критични ОТ системи (SCADA, DCS, ICS);

г) демилитаризирани зони (DMZ) за комуникација со надворешни мрежи.

1.2 Периметарска заштита:

а) Next-Generation Firewalls (NGFW) на сите мрежни граници;

б) Intrusion Detection/Prevention Systems (IDS/IPS);

в) Web Application Firewalls (WAF);

г) DDoS заштита.

1.3 Контрола на мрежен сообраќај:

а) политики за филтрирање помеѓу зони;
б) мониторинг на внатрешен сообраќај;
в) Network Access Control (NAC).
1.4 Далечински пристап:
а) VPN со силно шифрирање;
б) забрана на директен RDP, SSH или Telnet од интернет;
в) MFA за сите далечински пристапи;
г) временско ограничување на сесии.
2. КОНТРОЛА НА ПРИСТАП И УПРАВУВАЊЕ СО ИДЕНТИТЕТИ
2.1 Автентикација:
а) уникатни кориснички сметки;
б) политика за силни лозинки (минимум 12 карактери);
в) Заклучување на сметки по 3 неуспешни обиди; г)
MFA за привилегирани сметки и критични системи. Дополнително, за суштинските субјекти, за администраторски и критични ОТ улоги задолжително се применува фишинг-отпорна автентикација.
2.2 Авторизација:
а) принцип на најмала привилегија (Least Privilege);
б) Контрола на пристап базирана на улоги / Role-Based Access Control (RBAC);
в) Сегрегација на должности / Segregation of Duties;
г) редовен преглед на пристапни права.
2.3 Управување со привилегирани сметки (PAM):
а) централизирано управување;
б) Just-In-Time (JIT) привилегии;
в) снимање на привилегирани сесии;
г) автоматска ротација на лозинки.
2.4 Контрола на ОТ пристап:
а) посебни сметки за ОТ системи;
б) двојна авторизација /dual-authorization за критични промени;
в) физичка контрола на пристап до ОТ терминали.

3. УПРАВУВАЊЕ СО РАНЛИВОСТИ И ЗАКРПИ
3.1 Управување со ранливости:
а) месечно автоматизирано скенирање за ИТ, се препорачува квартално пасивно или активно скенирање за ОТ, согласно можностите.
б) приоритизација по CVSS (Critical 9.0-10.0, High 7.0-8.9, Medium 4.0-6.9, Low 0.1-3.9); в) рокови за ремедијација: за суштински субјекти — Critical 72 часа, High 14 дена, Medium 60 дена, Low 180 дена; за важни субјекти — Critical 7 дена, High 30 дена, Medium 90 дена, Low 180 дена. Покрај CVSS, субјектите задолжително ги отстрануваат ранливостите за кои е познато дека активно се експлоатираат, користејќи признати каталози на експлоатирани ранливости (CISA KEV или еквивалент), со примена на најкраткиот рок од овие каталози.
3.2 Управување со закрпи / Patch Management:
а) следење безбедносни билтени;
б) тестирање во изолирано опкружување;
в) планирани прозорци за одржување на ОТ системи;
г) rollback процедури за враќање.
3.3 Legacy системи:

а) дополнителна мрежна изолација;
б) зајакнат мониторинг;
в) Application Whitelisting;
г) план за евенуална можна замена.

4. СИСТЕМИ ЗА СЛЕДЕЊЕ И ОТКРИВАЊЕ
4.1 SIEM:
а) собирање логови од сите критични системи;
б) корелација на настани;
в) автоматски алерти;
г) чување безбедносни логови минимум 12 месеци. За пократко чување на други категории логови потребно е документирано образложение.
4.2 Endpoint Detection and Response (EDR):
а) на сите крајни точки (ИТ);
б) мониторинг на ОТ терминали.
4.3 Threat Intelligence:
а) следење на CERT билтени;
б) IOC споделување;
в) интеграција со SIEM.

5. КРИПТОГРАФИЈА И ШИФРИРАЊЕ
5.1 Шифрирање на податоци. Шифрирањето се применува врз основа на класификацијата на податоците и проценката на ризик, приоритетно за лични податоци, акредитиви и критични оперативни параметри.:
а) Data at Rest — AES-256 за бази на податоци, бекапи, критични фајлови;
б) Data in Transit — TLS 1.3+ за сите мрежни комуникации.
5.2 Управување со криптографски клучеви: а) централизирано управување; б) ротација согласно политика; в) безбедно чување (HSM за суштински субјекти).

6. БЕЗБЕДНОСТ НА IoT И ОТ СИСТЕМИ
6.1 IoT: а) инвентар на сите IoT уреди; в) мрежна сегментација; г) мониторинг; д) план за престанок на користење и отстранување на неподдржани уреди.
6.2 ОТ (SCADA/DCS/ICS): а) мрежна изолација; б) мониторинг на ОТ протоколи; в) change management; г) физичка безбедност на ОТ терминали.

7. ЗАЈАКНУВАЊЕ И БЕЗБЕДНИ КОНФИГУРАЦИИ
7.1 Зајакнување (промена default credentials, оневозможување непотребни сервиси) и имплементација на безбедни конфигурации применливи кај ИТ, ОТ и IoT.
7.2 Безбеден развој на софтвер (Secure SDLC-Software Development Life Cycle): Регулираните субјекти кои самостојно развиваат или значително модифицираат софтвер применуваат: (а) моделирање закани (threat modeling) во дизајн фазата; (б) безбедносен преглед на код (code review); (в) автоматизирано SAST/DAST скенирање; (г) скенирање на зависности (dependency/SCA); (д) безбедносни тестови пред продукциско пуштање. Кога субјектот не развива софтвер, овие барања се пренесуваат на добавувачите преку договорни клаузули.

8. ФИЗИЧКА БЕЗБЕДНОСТ НА ИКТ И ОТ СИСТЕМИ
8.1 Контрола на физички пристап: а) контролиран пристап до серверски соби и ОТ објекти; б) евиденција на влезови; в) видео надзор на критични локации.

8.2 Заштита од природни закани: а) противпожарна заштита; б) климатизација; в) резервно напојување (UPS, генератори).

ПРИЛОГ 2

ОРГАНИЗАЦИСКИ МЕРКИ ЗА САЈБЕР БЕЗБЕДНОСТ

Согласно член 12 од овие Правила, следува листа на Организациски мерки за сајбер безбедност кои регулираните субјекти се должни да ги имплементираат

1. ПОЛИТИКИ И ПРОЦЕДУРИ

1.1 Политика за сајбер безбедност: а) визија и цели; б) обем и примена; в) улоги и одговорности; г) одобрена од органот на управување. Политиката за сајбер безбедност задолжително ја адресира секоја категорија на мерки дефинирана во овие Правила и нивните Прилози.

1.2 Процедури: а) за управување со инциденти; б) за управување со пристап; в) за промени; г) за резервни копии; д) за набавка на ИКТ/ОТ.

1.3 Преглед од страна на раководство: политиките и процедурите се прегледуваат и ажурираат најмалку еднаш годишно.

2. УПРАВУВАЊЕ СО СРЕДСТВА

2.1 Инвентар: а) хардвер; б) софтвер; в) мрежни уреди; г) ОТ уреди; д) IoT уреди; (ѓ) управување со ранливости и закрпи; (е) управување со безбедни конфигурации и мониторинг. Инвентарот задолжително содржи: производител, верзија, локација. Се ажурира квартално.

2.2 Класификација: критичност според влијание врз услуги.

2.3 Животен циклус: Процес за управување со животен циклус: документирани процедури за безбедна набавка, инсталација, конфигурација, оперативности и користење, одржување и повлекување/уништување на ИКТ и ОТ средства, вклучувајќи безбедно бришење на податоци пред уништување.

3. УПРАВУВАЊЕ СО ПРОМЕНИ

3.1 Раководството одобрува промени на критични системи.

3.2 Процедура: барање, проценка на ризик, одобрување, тестирање, имплементација, верификација.

3.3 Emergency changes: поедноставена процедура со ретроактивно одобрување.

ПРИЛОГ 3

БЕЗБЕДНОСТ НА ЛАНЕЦОТ НА СНАБДУВАЊЕ

Согласно член 13 од овие Правила, Согласно член 12 од овие Правила, следува листа на мерки за сајбер безбедност поврзани со безбедност на ланецот на снабдување, кои регулираните субјекти се должни да ги имплементираат

1. ПРОЦЕНКА НА ДОБАВУВАЧИ

1.1 Due diligence: а) безбедносни сертификации (на пр. ISO 27001, SOC 2); б) историја на инциденти; в) безбедносни практики и процедури.

1.2 Критериуми: регулираните субјекти ја имаат предвид ранливоста специфична за секој добавувач, квалитетот на производите и сајбер безбедносната пракса, согласно член 32 став (4) од ЗБМИС.

1.3 Категоризација: критични, важни, стандардни добавувачи.

2. ДОГОВОРНИ БЕЗБЕДНОСНИ БАРАЊА

2.1 Задолжителни клаузули: а) известување за ранливости; б) безбедносни ажурирања; в) право на ревизија; г) инцидентно известување; д) end-of-life политика; (ѓ) барања за складирање, обработка и безбедно уништување/враќање на податоци; (е) доказ за обука за сајбер безбедност на вработените кај добавувачот; (ж) достапност на логови за безбедносен мониторинг; (з) стандарди за шифрирање конзистентни со Прилог 1, Дел 5.

2.2 SLA: безбедносни метрики, времиња за одговор, казнени одредби.

3. ОБЛАК УСЛУГИ И АУТСОРСИНГ

3.1 Cloud: а) SLA со безбедносни метрики; б) шифрирање (Bring Your Own Key — BYOK); в) локација на податоци; г) compliance проверка.

3.2 Аутсорсинг на безбедносни услуги: јасна поделба на одговорности; мониторинг на услуги.

4. ГОДИШНА ПРЕОЦЕНКА

4.1 Критичните добавувачи (добавувачи поврзани со критична инфраструктура кај регуларниот субјект) се преоценуваат најмалку еднаш годишно.

4.2 Извештајот за безбедност на ланецот на снабдување е дел од годишниот извештај.

ПРИЛОГ 4

УПРАВУВАЊЕ СО САЈБЕР БЕЗБЕДНОСНИ ИНЦИДЕНТИ

Согласно членови 14 и 15 од овие Правила, следува листа на мерки за управување со сајбер безбедносни инциденти кои регулираните субјекти се должни да ги имплементираат

1. МАТРИЦА ЗА КЛАСИФИКАЦИЈА НА ИНЦИДЕНТИ

КРИТИЧНО (P1) — Значаен инцидент: целосен прекин на критични енергетски услуги; компромитација на SCADA/DCS/ICS; ransomware на критични системи; прекугранично влијание.

ВИСОКО (P2) — Значаен инцидент: делумен прекин на услуги; неовластен пристап до критични системи; значителна финансиска штета; домино ефекти кон други субјекти.

СРЕДНО (P3) — Обичен инцидент: компромитација на некритични системи; успешен phishing без критично влијание; ранливост со потенцијал за ескалација.

НИСКО (P4) — Обичен инцидент: неуспешни напади; скенирање; минимално влијание.

ИНФОРМАТИВНО (P0) – Избегнати инциденти и индикатори без непосредно влијание и нарушување

2. ШАБЛОН: ФАЗА 1 — ИНИЦИЈАЛНО ИЗВЕСТУВАЊЕ (3 часа)

Идентификација на субјект (назив, регистарски број)

Службеник за сајбер безбедност (име, контакт)

Датум и време на откривање

Тип на инцидент/закана

Засегнати услуги и системи

Прелиминарна проценка на влијание

Информации за можно прекугранично влијание

3. ШАБЛОН: ФАЗА 2 — РАНО ПРЕДУПРЕДУВАЊЕ (24 часа)

Ажурирани информации од Фаза 1

Проценка дали инцидентот е предизвикан од незаконско или злонамерно дејствување

Проценка за можно прекугранично влијание

Категорија и ниво на сериозност

Преземени мерки за ограничување и мерки за отстранување

4. ШАБЛОН: ФАЗА 3 — ДЕТАЛНО ИЗВЕСТУВАЊЕ (72 часа)

Ажурирани информации од Фаза 2

Почетна проценка на сериозноста и влијанието

Показатели за загрозеност (IOCs)

Детален опис и временска рамка (timeline)

Вектор на напад

Статус на инцидентот

Мапирање на тактики, техники и подтехники според MITRE ATT&CK (за OT инциденти задолжително се користи MITRE ATT&CK for ICS матрицата); ниво на доверба во индикаторите.

5. ШАБЛОН: ФАЗА 4 — ЗАВРШНО ИЗВЕСТУВАЊЕ (1 месец)

Детален опис на инцидентот вклучувајќи сериозност и влијание

Тип на закана или главна причина

Мерки за ублажување што се примениле и се применуваат

Прекугранично влијание доколку е соодветно

Анализа на основна причина (Root Cause Analysis)

Научени лекции (Lessons Learned)

Препораки и план за имплементација

6. ШАБЛОН: ИЗВЕШТАЈ ЗА НАПРЕДОК

Се доставува доколку инцидентот е во тек при поднесување на завршното известување. Содржи: ажуриран статус; преземени мерки; очекувано времетраење; потребна поддршка.

ПРИЛОГ 5

МЕТОДОЛОГИЈА ЗА ПРОЦЕНКА НА РИЗИЦИ

Согласно член 8 од овие Правила, регулираните субјекти имаат обврска да ја применуваат следната Методологија за проценка на ризици.

1. РАМКА ЗА УПРАВУВАЊЕ СО РИЗИЦИ

1.1 Методологијата треба да е заснована на ISO/IEC 27005 и е усогласена со барањата на ЗБМИС чл.32 ст.3 т.1.

1.2 Фази: Контекст и опфат → Идентификација → Анализа → Евалуација → Третман → Мониторинг → Комуникација.

1.3 Органот на управување ја усвојува годишната проценка на ризици согласно чл.31 ст.1 од ЗБМИС.

2. ИДЕНТИФИКАЦИЈА НА СРЕДСТВА, ЗАКАНИ И РАНЛИВОСТИ

2.1 Средства: ИТ системи, OT системи (SCADA, DCS, ICS), мрежна инфраструктура, IoT уреди, податоци, физичка инфраструктура, човечки ресурси.

2.2 Закани: природни катастрофи, технички дефекти, човечки грешки, злонамерни активности (APT, ransomware, DDoS, insider threat, supply chain attack).

2.3 Ранливости: технички (софтверски, хардверски, мрежни), организациски (процедурални, компетенциски), физички.

3. МАТРИЦА НА РИЗИЦИ

3.1 Регулираниот субјект самостојно ја дефинира матрицата на ризици, со најмалку три нивоа на веројатност и влијание. Препорачано е користење на матрица на ризици со 5 (пет) нивоа на веројатност и влијание:

Веројатност (5 нивоа): Многу ниска (1), Ниска (2), Средна (3), Висока (4), Многу висока (5).

Влијание (5 нивоа): Незначително (1), Мало (2), Средно (3), Сериозно (4), Критично (5).

3.2 Ниво на ризик = Веројатност × Влијание. Категории: Низок (1-6), Среден (7-12), Висок (13-19), Критичен (20-25).

4. СТРАТЕГИИ ЗА ТРЕТМАН

4.1 Прифаќање (Accept) — за ризици под прагот на толеранција.

4.2 Ублажување (Mitigate) — имплементација на контроли.

4.3 Пренесување (Transfer) — осигурување, аутсорсинг.

4.4 Избегнување (Avoid) — елиминација на изворот на ризик.

СТРУКТУРА НА РЕГИСТАР НА РИЗИЦИ

Регулираните субјекти се должни да водат Регистар на ризици во следниот формат и со следните податоци.

ID | Опис | Категорија | Средства | Закани | Ранливости | Веројатност | Влијание | Ниво | Контроли | Остаточен ризик | Стратегија | Одговорно лице | Рок | Статус

ПРИЛОГ 6

СТАНДАРДИ ЗА САЈБЕР БЕЗБЕДНОСТ
ВО ЕНЕРГЕТИКАТА

Согласно член 9 од овие Правила, регулираните субјекти се должни да ги имплементираат и користат следните стандарди.

1. ЗАДОЛЖИТЕЛНИ СТАНДАРДИ

1.1 ISO/IEC 27001:2022 — Систем за управување со безбедноста на информациите (ISMS). Задолжителна сертификација за суштинските субјекти.

1.2 ISO/IEC 27002:2022 — Контроли за безбедноста на информациите. Референтна рамка за имплементација.

2. ПРЕПОРАЧАНИ СТАНДАРДИ

2.1 ISO/IEC 27005:2022 — Управување со ризици за безбедноста на информациите.

2.2 ISO/IEC 27019:2017 — Контроли за енергетскиот сектор.

2.3 IEC 62443 — Безбедност на индустриски комуникациски мрежи и системи.

2.4 ISO 22301 — Систем за управување со деловен континуитет.

2.5 NIST Cybersecurity Framework (CSF) 2.0 — Рамка за управување со сајбер ризици.

3. СЕРТИФИКАЦИЈА НА ИКТ ПРОИЗВОДИ

3.1 Регулираните субјекти може да бараат ИКТ производите и услугите да поседуваат сертификати издадени согласно европски шеми за сертификација на сајбер безбедноста, согласно член 35 од ЗБМИС.

ПРИЛОГ 7

МЕТОДОЛОГИЈА ЗА КЛАСИФИКАЦИЈА НА САЈБЕР БЕЗБЕДНОСНИ ИНЦИДЕНТИ ВО ЕНЕРГЕТСКИОТ СЕКТОР

Согласно член 14 став (3) и член 33 став (12) од ЗБМИС, Регулаторната комисија за енергетика, водни услуги и услуги за управување со комунален отпад на Република Северна Македонија ја усвои следната Методологија за класификација на сајбер безбедносни инциденти во енергетскиот сектор, како составен дел на овие Правила.

1. ПРЕДМЕТ И ПРАВНА ОСНОВА

1.1 Оваа методологија ги утврдува поблиските критериуми и прагови за определување на обични и значајни сајбер безбедносни инциденти во енергетскиот сектор, согласно член 33 став (12) од Законот за безбедност на мрежни и информациски системи.

1.2 Регулаторната комисија за енергетика, водни услуги и услуги за управување со комунален отпад на Република Северна Македонија ја донесува оваа методологија по претходна согласност од Министерството за дигитална трансформација.

1.3 Методологијата е усогласена со Имплементирачката регулатива (EU) 2024/2690 за критериуми за значајни инциденти, и се применува како дополнение на членот 14 и членот 15 од овие Правила.

2. ДЕФИНИЦИИ

2.1 „Значаен сајбер безбедносен инцидент" е инцидент кој исполнува барем еден од критериумите наведени во точка 4 од оваа методологија.

2.2 „Обичен сајбер безбедносен инцидент" е инцидент кој не исполнува ниту еден критериум за значајност.

2.3 „Избегнат инцидент" (near-miss) е настан кој можел да биде инцидент, но е спречен со контролните мерки.

2.4 „Инцидент со голем опфат" е значаен инцидент кој влијае на два или повеќе регулирани субјекти или има прекугранично влијание.

3. ПРИНЦИПИ

3.1 Мулти-критериумски пристап: Инцидент е значаен ако исполнува барем еден критериум за значајност (принцип „или").

3.2 Претпазливост: При сомнеж, инцидентот се третира како значаен.

3.3 Пропорционалност: Праговите за суштински и важни субјекти се различни, одразувајќи ги нивните различни ресурси и влијание.

3.4 Динамичност: Класификацијата може да се промени во текот на инцидентот — обичен може да стане значаен, но значаен не може да се деградира во обичен по започнато известување.

3.5 ОТ приоритет: Секој потврден неовластен пристап до ОТ/SCADA систем кој контролира физички процес во енергетскиот сектор автоматски се класифицира како значаен.

4. КРИТЕРИУМИ ЗА ЗНАЧАЈНОСТ

Инцидент е ЗНАЧАЕН ако исполнува барем еден од следниве критериуми:

К1 — НАРУШУВАЊЕ НА УСЛУГИ: Инцидентот предизвикал целосен или делумен прекин на услуги на регулираниот субјект. Праг за суштински субјект: прекин ≥ 1 час на критична услуга, или деградирање ≥ 25% на капацитетот во траење ≥ 4 часа. Праг за важен субјект: прекин ≥ 4 часа на критична услуга, или деградирање ≥ 50% на капацитетот во траење ≥ 8 часа.

К2 — ЗАСЕГНАТИ КОРИСНИЦИ: Инцидентот засегнал физички или правни лица — корисници на услугите на субјектот. Праг за регулираните субјекти: ≥ 10.000 корисници или ≥ 5% од вкупниот број на снабдувани корисници, за време траење он најмалку 1 час.

К3 — ФИНАНСИСКИ ЗАГУБИ: Инцидентот предизвикал директни или индиректни финансиски загуби. Праг за суштински субјект: ≥ 100.000 EUR или ≥ 1% од годишниот приход (кое е помало). Праг за важен субјект: ≥ 500.000 EUR или ≥ 5% од годишниот приход (кое е помало).

К4 — КОМПРОМИТАЦИЈА НА ПОДАТОЦИ

К4.1 — Лични податоци. Повредата на безбедноста на лични податоци (неовластен пристап, губиток, неовластено откривање, измена или уништување на лични податоци) кај регулиран субјект во својство на контролор или обработувач примарно се управува согласно Законот за заштита на личните податоци Овие обврски се исполнуваат паралелно и независно од обврските за пријавување значајни сајбер безбедносни инциденти по овие Правила.

Повредата на лични податоци се третира како значаен сајбер безбедносен инцидент по овие Правила (со активирање на четирифазно известување до Регулаторната комисија за енергетика и MKD-CIRT) кога е исполнет некој од следниве прагови:

· ≥ 100 субјекти на лични податоци за суштински субјект;

· ≥ 1.000 субјекти на лични податоци за важен субјект;

· компромитација на криптографски клучеви, акредитиви или сертификати кои штитат лични податоци — автоматски значаен.

Регулаторната комисија за енергетика и MKD-CIRT ја координираат обработката на инциденти кои истовремено претставуваат и повреда на безбедноста на личните податоци со Агенцијата за заштита на личните податоци.

К4.2 — Критични оперативни и деловни податоци. Неовластен пристап, губиток, неовластено откривање, измена или уништување на податоци кои не се лични податоци, а се критични за функционирањето на регулираниот субјект, сигурноста на снабдување, пазарната отчетност или регулаторното известување.

Категории на критични оперативни податоци за енергетскиот сектор:

а) податоци од SCADA/EMS/DMS (телеметрија, поставувачки вредности, алармни логови);

б) пазарни и податоци за порамнување (settlement, balancing, NEMO трансакции, билатерални договори);

в) податоци за мерење и наплата (billing, metering, архиви од паметни мерачи);

г) конфигурациски податоци за мрежата и заштитните системи (топологија, заштитни параметри, GIS податоци за критична инфраструктура);

д) резервни копии на критични системи и нивните криптографски клучеви.

Праг за значајност (применлив на двата типа субјекти, освен каде е изречно поинаку):

· секоја потврдена компромитација на доверливост, интегритет или достапност на податоци од категориите а), г) и д) — автоматски значаен инцидент;

· неовластена измена или уништување на податоци од категорија б) — автоматски значаен инцидент;

· губиток, неовластено откривање или неовластена измена на податоци за наплата/мерење од категорија в): ≥ 10.000 записи или ≥ 5% од корисничката база за суштински субјект, односно ≥ 100.000 записи или ≥ 10% од корисничката база за важен субјект.

· Компромитација на криптографски клучеви, сертификати или акредитиви кои штитат која било од горенаведените категории на оперативни податоци — секогаш значаен инцидент, без оглед на обемот.

К5 — ПРЕКУГРАНИЧНО ВЛИЈАНИЕ: Инцидентот влијае или може да влијае на ентитети, услуги, сектори или корисници во други држави. Секое потврдено или веројатно прекугранично влијание е автоматски значаен инцидент, согласно член 33 став (1) од ЗБМИС.

К6 — OT/SCADA КОМПРОМИТИРАЊЕ: Неовластен пристап, контрола или нарушување на OT/SCADA/EMS/DCS систем кој контролира физички процес во енергетскиот сектор. Овој инцидент е автоматски значаен за сите субјекти, без разлика на класификацијата.

К7 — МРЕЖНА СТАБИЛНОСТ: Инцидентот предизвикал влијание врз фреквенцијата, напонот, балансирањето или N-1 критериумот на електроенергетскиот систем. Праг: загуба ≥ 50 MW генерација или товар; фреквентна девијација > ±200 mHz; напонско одстапување > ±10% од номинална вредност.

К8 — ПРЕКИН НА СНАБДУВАЊЕ СО ЕНЕРГИЈА: Инцидентот предизвикал прекин на пренос, дистрибуција или снабдување со електрична енергија или природен гас. Праг за суштински субјект: ≥ 5.000 домаќинства без снабдување ≥ 1 час, или ≥ 1.000 домаќинства без снабдување ≥ 4 часа. Праг за важен субјект: ≥ 10.000 домаќинства без снабдување ≥ 2 часа.

К9 — ФИЗИЧКА БЕЗБЕДНОСТ: Инцидентот предизвикал или може да предизвика загрозување на живот, здравје или околина. Автоматски значаен за сите субјекти. Доколку потврдено физичко безбедносно влијание е очигледно при откривање, инцидентот автоматски ќе се третира како значаен. Дополнително, секое влијание врз снабдувањето со енергија на болници, итни служби (ИМП, противпожарни единици, полиција), системи за водоснабдување или јавни електронски комуникациски мрежи се класифицира како значаен инцидент, без оглед на бројот на засегнати домаќинства.

К10 — КАСКАДНИ/ДОМИНО ЕФЕКТИ: Инцидентот може да предизвика ланчана реакција кај други регулирани субјекти или други сектори. Праг: потврдено или веројатно каскадно влијание на ≥ 1 друг регулиран субјект (суштински) или ≥ 2 (важен).

К11 — ГУБЕЊЕ НА ЕЛЕКТРИЧНА ЕНЕРГИЈА: Загуба на електрична енергија ≥ 50 MWh во временска рамка од 24 часа како директен резултат на сајбер инцидент е автоматски значаен инцидент, без разлика на класификацијата на субјектот.

5. АВТОМАТСКА КЛАСИФИКАЦИЈА (OT/SCADA)

5.1 Следниве настани АВТОМАТСКИ се класифицираат како значајни инциденти без потреба од проценка по критериумите:

а) Потврден неовластен пристап до SCADA/EMS/DCS систем кој контролира физички процес (генерација, пренос, дистрибуција, складирање, пренос/дистрибуција на гас);

б) Неовластена промена на конфигурација, или заштитни параметри на OT систем;

в) Детекција на малвер специфично дизајниран за ICS/SCADA;

г) Комуникација од OT мрежа кон познат Command & Control (C2) сервер;

д) Нарушување на мрежната сегментација помеѓу ИТ и OT мрежата (lateral movement од ИТ во OT);

ѓ) Компромитирање на работни станици за управување и пристап за OT систем;

е) Неовластен далечински пристап (VPN, jump server) до OT мрежа.

6. ПОСТАПКА ЗА КЛАСИФИКАЦИЈА

6.1 Чекор 1 — Детекција и тријажа: Службеникот за сајбер безбедност или тимот за одговор го потврдува постоењето на инцидентот и определува дали е ИТ, ОТ или комбиниран.

6.2 Чекор 2 — Автоматска проверка: Ако инцидентот спаѓа во точка 5 (автоматска класификација) → ЗНАЧАЕН → активирање на 4-фазно известување.

6.3 Чекор 3 — Проценка по критериуми: Проценка на К1-К10 критериумите со достапните информации. Ако барем еден критериум е исполнет → ЗНАЧАЕН. Ако ниту еден не е исполнет → ОБИЧЕН.

6.4 Чекор 4 — Принцип на претпазливост: Ако информациите се недоволни за проценка, инцидентот се третира како значаен.

6.5 Чекор 5 — Активирање на известување: За значајни инциденти — 4-фазно известување согласно член 15 од Правилата. За обични — евидентирање и квартално известување.

6.6 Чекор 6 — Рекласификација: Обичен инцидент може да се рекласифицира во значаен ако во текот на истрагата се утврди дека е исполнет некој критериум. Значаен инцидент НЕ МОЖЕ да се деградира во обичен по започнато известување.

7. ПОСЕБНИ ПРАВИЛА

7.1 Ransomware: Секој ransomware напад кој ги засегнува ОТ системите или критичните ИТ системи за управување со енергетскиот систем автоматски е значаен инцидент.

7.2 Ланец на снабдување (Supply Chain): Компромитирање на софтверски ажурирања или хардвер од добавувач кој снабдува 2 (два) или повеќе регулирани субјекти е значаен инцидент.

7.3 Внатрешна закана (Insider Threat): Намерно дејствување на вработен или поранешен вработен кое резултира со неовластен пристап до критични системи е значаен инцидент.

7.4 Нулта-ден (Zero-day): Активна експлоатација на нулта-ден ранливост во критичен систем е значаен инцидент.

7.5 Координиран напад: Симултани или координирани напади на 2 (два) или повеќе регулирани субјекти се значаен инцидент со голем опфат, без оглед на индивидуалното влијание.

8. АЖУРИРАЊЕ НА МЕТОДОЛОГИЈАТА

8.1 Регулаторната комисија за енергетика ја ажурира Методологијата најмалку еднаш годишно или по секој значаен инцидент кој укажува на потреба од прилагодување на прагови или критериуми.

8.2 Ажурирањето се врши по претходна согласност од Министерството за дигитална трансформација, согласно член 33 став (12) од ЗБМИС.

8.3 При ажурирање, Регулаторната комисија за енергетика, водни услуги и услуги за управување со комунален отпад на Република Северна Македонија ги зема предвид: (а) трендовите на инциденти во енергетскиот сектор; (б) нови типови закани и ранливости; (в) препораките на ENISA и надлежниот CSIRT; (г) искуствата на регулираните субјекти.

8.4 Регулираните субјекти и MKD-CIRT се консултираат пред секоја измена на методологијата.