Врз основа на член 23 став (6), а во врска со член 23 став (3), член 23 став (1), член 11 став (1) точка 2), член 16 став (1), член 20 став (1) и член 24 од Законот за безбедност на мрежни и информациски системи („Службен весник на Република Северна Македонија" бр. 135/2025), на предлог на Националниот центар за одговор на компјутерски инциденти (MKD-CIRT), директорот на Агенцијата за електронски комуникации донесе

МЕТОДОЛОГИЈА

за спроведување на анализа на ризик за приоритизација на обврските на Националниот центар за одговор на компјутерски инциденти (MKD-CIRT)

I. ОПШТИ ОДРЕДБИ

Член 1
(Предмет)

(1) Со оваа методологија се уредува начинот на спроведување на анализата на ризик заради приоритизација на обврските на Националниот центар за одговор на компјутерски инциденти (во натамошниот текст: MKD-CIRT), при извршување на задачите од член 23 став (1) од Законот за безбедност на мрежни и информациски системи (во натамошниот текст: Законот).

(2) Оваа методологија претставува оперативен и методолошки инструмент за распределба на расположливите човечки, технички и организациски ресурси на MKD-CIRT во случаи кога повеќе задачи, пријави, инциденти, закани, ранливости или барања за поддршка треба да се обработуваат истовремено.

(3) Методологијата не уредува класификација на суштински и важни субјекти, ниту прагови за определување на обични и значајни сајбер безбедносни инциденти, кои се уредуваат со посебни акти согласно Законот.

Член 2
(Цел)

Целта на оваа методологија е да обезбеди законито, доследно, проверливо и пропорционално приоритизирање на задачите на MKD-CIRT, така што највисок приоритет имаат задачите кои се поврзани со значајни сајбер безбедносни инциденти, значајни сајбер закани, инциденти со голем опфат, прекугранично влијание, критични услуги, суштински и важни субјекти и ризици со потенцијал за сериозно влијание врз безбедноста на мрежните и информациските системи.

Член 3
(Применливост)

(1) Оваа методологија се применува при извршување на задачите на MKD-CIRT од член 23 став (1) од Законот, особено кога истовремено постојат повеќе оперативни обврски и кога е потребно да се утврди редослед, ниво на итност, распределба на ресурси или ескалација.

(2) Методологијата не може да се примени на начин кој би довел до неизвршување или одложување на императивни законски обврски, особено роковите за известување и постапување утврдени со Законот.

(3) При примената на методологијата, MKD-CIRT ги зема предвид релевантните европски и меѓународни стандарди, добри практики и технички насоки за CSIRT работење, управување со инциденти, анализа на ризик и безбедна размена на информации, доколку истите не се спротивни на Законот и на националните акти.

Член 4

(Начела)

1) законитост — приоритизацијата се врши во рамките на надлежностите на MKD-CIRT и не смее да дерогира законски рокови и обврски;
2) заштита на јавниот интерес — предност имаат задачите кои спречуваат или ублажуваат сериозно влијание врз јавната безбедност, јавната заштита, јавното здравје, економијата, демократскиот систем, животната средина или националната безбедност;
3) ризик-базиран пристап — приоритетот се утврдува врз основа на влијание, веројатност, итност и можност за ескалација;
4) пропорционалност — ресурсите се распределуваат сразмерно на сериозноста, опфатот и очекуваното влијание;
5) недискриминација и еднаков третман — споредливи случаи се оценуваат според исти критериуми;
6) документираност и проверливост — секоја одлука за приоритизација мора да биде образложена и евидентирана;
7) координација — приоритизацијата се спроведува во координација со Министерството за дигитална трансформација, други надлежни органи и тимови за одговор на компјутерски инциденти, кога тоа е потребно;
8) доверливост и минимизација — информациите се користат само во обем неопходен за проценка, постапување и известување.

Член 5

(Однос со стандардизираните практики по член 23 став (5) од Законот)

(1) Оваа методологија се применува во согласност со заедничките или стандардизирани практики, шеми за класификација и класификации кои ги утврдува MKD-CIRT согласно член 23 став (5) од Законот, особено во делот на:

1) процедури за справување со инциденти;
2) управување со кризи;
3) координирано откривање на ранливости;
4) таксономија на инциденти, сериозност, влијание, TLP ознаки и оперативни статуси;
5) правила за безбедна размена на информации меѓу тимовите за одговор на компјутерски инциденти.

(2) Доколку по донесувањето на оваа методологија MKD-CIRT утврди или измени стандардизирани практики и класификации согласно член 23 став (5) од Законот, оваа методологија се применува на начин што обезбедува нивна меѓусебна кохерентност.

II. КАТЕГОРИИ НА ОБВРСКИ И ПРАВЕН ПРИОРИТЕТ

Член 6

(Категории на задачи што може да се приоритизираат)

Предмет на приоритизација согласно оваа методологија се задачите на MKD-CIRT утврдени со член 23 став (1) од Законот, и тоа:

1) следење и анализа на сајбер закани, ранливости и инциденти кај субјектите од надлежност на MKD-CIRT;

2) доставување рани предупредувања, најави, соопштенија и информации за сајбер закани, ранливости и инциденти;

3) обезбедување одговор на инциденти и помош на суштински и важни субјекти, надлежни органи и други засегнати страни;

4) собирање и анализа на форензички податоци, динамична анализа на ризици и инциденти и информирање за состојбите во сајбер безбедноста;

5) проактивно ненаметливо скенирање на јавно достапни мрежни и информациски системи на субјектите од надлежност;

6) известување на субјектите за резултатите од проактивното скенирање;

7) учество во Мрежата на тимови за одговор на компјутерски инциденти и обезбедување взаемна помош;

8) придонес за користење на алатки за безбедносна размена на информации;

9) координација во процесот на координирано откривање на ранливости согласно член 24 од Законот.

Член 7

(Класи на обврски според правен и оперативен карактер)

(1) За потребите на оваа методологија, задачите и обврските се категоризираат во три класи:

Класа	Опис
Класа I — императивни и временски критични обврски	Обврски кои произлегуваат директно од Законот, врзани се со законски рок, значаен инцидент, значајна сајбер закана, прекугранично влијание, инцидент со голем опфат, сајбер криза или непосредна опасност за критична услуга.
Класа II — оперативни обврски со висок ризик	Обврски поврзани со активни инциденти, ранливости со висок потенцијал за експлоатација, барања за техничка поддршка од суштински или важни субјекти, CVD случаи со значително влијание и задачи од Мрежата на CSIRT со јасен ризик.
Класа III — редовни, аналитички и поддржувачки обврски	Редовно следење, анализа на трендови, подготовка на едукативни и аналитички продукти, поддршка на алатки за размена на информации, рутински скенирања и други задачи без непосредна временска критичност.

(2) Обврските од Класа I имаат предност пред обврските од Класа II и Класа III. Во рамките на иста класа, приоритетот се определува според оценката на ризик утврдена со оваа методологија.

III. РАМКА ЗА ОЦЕНКА НА РИЗИК

Член 8

(Модел за оценување)

(1) Оценката на ризик за приоритизација се врши преку комбинација на два основни фактори:

1) влијание (I) — последици што може да настанат ако задачата не се обработи навремено или со соодветен капацитет;

2) веројатност (V) — веројатност дека ризикот ќе се реализира, ќе ескалира или ќе предизвика дополнителна штета доколку не се постапи навремено.

(2) Резултатот на ризик се пресметува според формулата:

$$R = I \times V$$

(3) Влијанието и веројатноста се оценуваат на скала од 1 до 5, а резултатот на ризик се движи од 1 до 25.

Член 9

(Скала за влијание)

Ниво	Ознака	Опис
5	Критично	Потенцијал за сериозно нарушување на критична услуга, значаен инцидент со голем опфат, прекугранично влијание, непосредна опасност за јавна безбедност, јавна заштита, јавно здравје, национална безбедност, економија, демократски систем или човечки животи.
4	Високо	Потенцијал за значајно нарушување кај суштински субјект, важна инфраструктура, јавна услуга или повеќе засегнати субјекти, со можност за брза ескалација или значително материјално/нематеријално влијание.
3	Средно	Потенцијал за нарушување кај важен субјект, ограничено секторско или регионално влијание, или ризик кој може да ескалира доколку не се обработи во разумен рок.

2	Ниско	Локално или ограничено влијание кај еден субјект, без јасен потенцијал за каскадни последици.
1	Минимално	Информативно, едукативно или рутинско значење, без оперативно влијание врз континуитетот на услугите.

Член 10

(Критериуми за оценување на влијание)

1) дали задачата се однесува на значаен сајбер безбедносен инцидент, значајна сајбер закана, избегнат инцидент со висок потенцијал или инцидент со голем опфат;
2) дали се засегнати суштински субјекти, важни субјекти, јавни институции, критична инфраструктура или даватели на услуги од дигитална инфраструктура;
3) очекуваното влијание врз достапноста, интегритетот, автентичноста и доверливоста на мрежните и информациските системи;
4) бројот и видот на засегнати корисници, институции, правни лица или други субјекти;
5) можноста за каскадно ширење кон други субјекти, сектори, добавувачи или услуги;
6) постоење на прекугранично влијание или потреба од меѓународна координација;
7) можноста за повреда на лични податоци, деловни тајни, класифицирани информации или доверливи податоци;
8) влијание врз јавната безбедност, јавната заштита, јавното здравје, економијата, националната безбедност или довербата во дигиталните услуги;
9) законски рокови, обврски за известување и потреба од итно информирање на Министерството или други надлежни органи.

Член 11

(Скала за веројатност)

Ниво	Ознака	Опис
5	Многу висока	Активна експлоатација е во тек, постои потврдена закана со непосредно дејство, достапен е експлоит во употреба или инцидентот веќе се шири.
4	Висока	Постојат веродостојни докази за активна закана, јавен експлоит, кампања во тек кај партнерски субјекти или ранливост без доволно распространета корекција.
3	Средна	Постојат индикатори за подготовка на напад, релевантни разузнавачки

		информации, позната ранливост со потенцијал за експлоатација или значајна изложеност.
2	Ниска	Постои теоретска можност или ограничени индикатори, без докази за активна експлоатација или непосредна ескалација.
1	Многу ниска	Хипотетичка можност, ограничена применливост или целосно контролирани услови.

Член 12

(Критериуми за оценување на веројатност)

1) потврдена активна експлоатација или инцидент во тек;
2) постоење на јавен, комерцијален или широко достапен експлоит;
3) ниво на изложеност на засегнатите системи, особено интернет-достапност и изложени критични сервиси;
4) распространетост на ранливоста, недостиг на корекција или тешкотија за брзо ублажување;
5) релевантни индикатори за загрозеност, тактики, техники и процедури, кампањи или заканувачи;
6) претходна историја на слични инциденти кај истиот субјект, сектор или поврзани субјекти;
7) доверливост на изворот на информацијата и степен на потврденост на наодите;
8) можност ризикот да ескалира доколку MKD-CIRT не постапи без одлагање.

IV. МАТРИЦА ЗА ПРИОРИТИЗАЦИЈА И ДЕЈСТВА

Член 13

(Нивоа на приоритет)

Врз основа на резултатот R = I × V се утврдува следното ниво на приоритет:

Резултат R	Ниво на приоритет
1–4	**P1 — Низок**
5–8	**P2 — Среден**
9–12	**P3 — Висок**
13–19	**P4 — Многу висок**
20–25	**P5 — Критичен**

Член 14

(Матрица 5×5)

Влијание / Веројатност	V=1	V=2	V=3	V=4	V=5
I=5	P2	P3	P4	P5	P5
I=4	P2	P3	P3	P4	P5
I=3	P1	P2	P3	P3	P4
I=2	P1	P1	P2	P2	P3
I=1	P1	P1	P1	P2	P2

Член 15

(Дејства по ниво на приоритет)

Ниво	Оперативни дејства
P5 — Критичен	Непосредно активирање на расположливите ресурси; работа во континуиран режим; задолжително информирање на раководителот на MKD-CIRT и директорот на АЕК; без одлагање информирање на Министерството кога е применливо; разгледување на потреба за ескалација кон Тимот за координација согласно Законот.
P4 — Многу висок	Активирање на тим за справување или специјализирана поддршка; приоритетно распределување на ресурси; редовно информирање на раководителот на MKD-CIRT; координација со други тимови и надлежни органи кога е потребно.
P3 — Висок	Назначување одговорно лице или аналитичар; следење на состојбата; обработка во скратени оперативни рокови; ескалација ако се зголеми влијанието или веројатноста.
P2 — Среден	Обработка во рамките на редовните оперативни процедури и расположливи ресурси, со периодично преиспитување на приоритетот.
P1 — Низок	Обработка по редовен редослед, без влијание врз задачите од повисок приоритет; може да се одложи, групира или обработи аналитички ако не постои непосреден ризик.

V. ПОСТАПКА ЗА АНАЛИЗА И ПРИОРИТИЗАЦИЈА

Член 16

(Чекори на постапката)

1) идентификација на задачата, пријавата, инцидентот, заканата, ранливоста или барањето за поддршка;
2) проверка на правниот основ, законскиот рок и надлежноста на MKD-CIRT;
3) утврдување на класата на обврската согласно член 7 од оваа методологија;
4) прибирање на достапните факти, технички индикатори, информации од засегнатиот субјект, партнерски тимови или други извори;
5) оценување на влијанието согласно член 9 и член 10 од оваа методологија;
6) оценување на веројатноста согласно член 11 и член 12 од оваа методологија;
7) пресметка на резултатот на ризик и утврдување на ниво на приоритет;
8) распределба на ресурси, определување одговорно лице и временска рамка за постапување;
9) евидентирање на одлуката за приоритизација и кратко образложение;
10) периодично преиспитување на приоритетот кога ќе се појават нови информации или кога ќе се промени состојбата.

Член 17

(Одговорни лица)

(1) Анализата на ризик за приоритизација ја врши:

1) дежурниот аналитичар или старешината на смената — за тековни оперативни задачи и првична проценка;
2) раководителот на MKD-CIRT — за задачи со приоритет P4 и P5, за задачи со прекугранично влијание и за случаи со потреба од координација со други органи;
3) директорот на АЕК — за случаи со стратешко значење, потреба од дополнителни ресурси, меѓуинституционална координација или известување на повисоко ниво;
4) Тимот за координација — кога се исполнети условите за инцидент со голем опфат или сајбер безбедносна криза согласно Законот.

(2) Доколку постои несогласување во однос на приоритетот, се применува повисокото предложено ниво додека раководителот на MKD-CIRT не донесе конечна оперативна одлука.

Член 18

(Документирање)

(1) За секоја анализа на ризик за приоритизација се документираат најмалку следните податоци:

1) идентификација на задачата или инцидентот;
2) краток опис на фактичката состојба;
3) класа на обврската;
4) оценка на влијание и образложение;
5) оценка на веројатност и образложение;

6) резултат R и ниво на приоритет;

7) распределени ресурси и одговорни лица;

8) рокови, ескалации и известувања;

9) временски печат и идентитет на лицето кое ја извршило проценката;

10) подоцнежни промени на приоритетот и причините за промената.

(2) Документацијата од ставот (1) на овој член се води во оперативната евиденција на MKD-CIRT или во друг соодветен систем што го користи MKD-CIRT, согласно правилниците за евиденција и Националниот регистар на сајбер инциденти.

VI. ОДНОС КОН ЗАКОНСКИТЕ РОКОВИ И КАПАЦИТЕТИ

Член 19

(Почитување на законските рокови)

(1) Приоритизацијата согласно оваа методологија не може да биде основ за непочитување на законски утврдени рокови, обврски за известување, обврски за проследување информации или обврски за давање одговор и поддршка утврдени со Законот.

(2) Кога MKD-CIRT нема доволно ресурси за паралелно извршување на повеќе законски обврски, раководителот на MKD-CIRT без одлагање го известува директорот на АЕК и предлага мерки за обезбедување дополнителни ресурси, преуредување на внатрешната распределба или активирање на соработка со други тимови за одговор на компјутерски инциденти.

(3) Кога состојбата може да има пошироко национално, прекугранично или кризно значење, MKD-CIRT го информира Министерството за дигитална трансформација согласно Законот и применливите процедури.

Член 20

(Извештај за капацитетски ограничувања)

(1) Доколку примената на оваа методологија покаже повторлив или системски недостиг на капацитети за извршување на задачите на MKD-CIRT, раководителот на MKD-CIRT подготвува извештај до директорот на АЕК.

(2) Извештајот од ставот (1) на овој член содржи: број и вид на задачи кои биле одложени или обработени со намален капацитет, причини за ограничувањата, ризици за националната сајбер безбедност и предлог мерки за зајакнување на човечките, техничките и организациските капацитети.

VII. ПРЕИСПИТУВАЊЕ И УНАПРЕДУВАЊЕ

Член 21

(Периодично преиспитување)

(1) Оваа методологија се преиспитува најмалку еднаш годишно, како и по секој значаен сајбер безбедносен инцидент, инцидент со голем опфат или сајбер безбедносна криза кога примената на методологијата укажала на потреба од измена.

(2) Преиспитувањето се врши врз основа на оперативната статистика, научените поуки, повратните информации од субјектите и партнерските тимови, промените во заканите и промените во законската или подзаконската рамка.

(3) Предлог за изменување и дополнување на методологијата подготвува MKD-CIRT, а го доставува до директорот на АЕК.

VIII. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 22

(Оперативни обрасци)

(1) MKD-CIRT, во рок од 30 дена од денот на влегувањето во сила на оваа методологија, изготвува работни обрасци, контролни листи и електронски шаблони за практична примена на методологијата.

(2) Обрасците од ставот (1) на овој член се внатрешни оперативни документи и се ажурираат по потреба од страна на раководителот на MKD-CIRT.

Член 23

(Усогласување со постојните процедури)

(1) Постојните оперативни процедури на MKD-CIRT се усогласуваат со оваа методологија во рок од 60 дена од денот на нејзиното влегување во сила.

(2) До завршувањето на усогласувањето, постојните процедури се применуваат во делот во кој не се спротивни на Законот и на оваа методологија.

Член 24

(Влегување во сила)

Оваа методологија влегува во сила од денот на нејзиното објавување на веб страната на Агенцијата за електронски комуникации и MKD-CIRT.

Бр. 0101-1513/18

14.07. 2026 година

Скопје

Директор

на Агенцијата за електронски комуникации

Nusret Haliti

Изготвил:

Раководител на MKD-CIRT
Sevdali Selmani