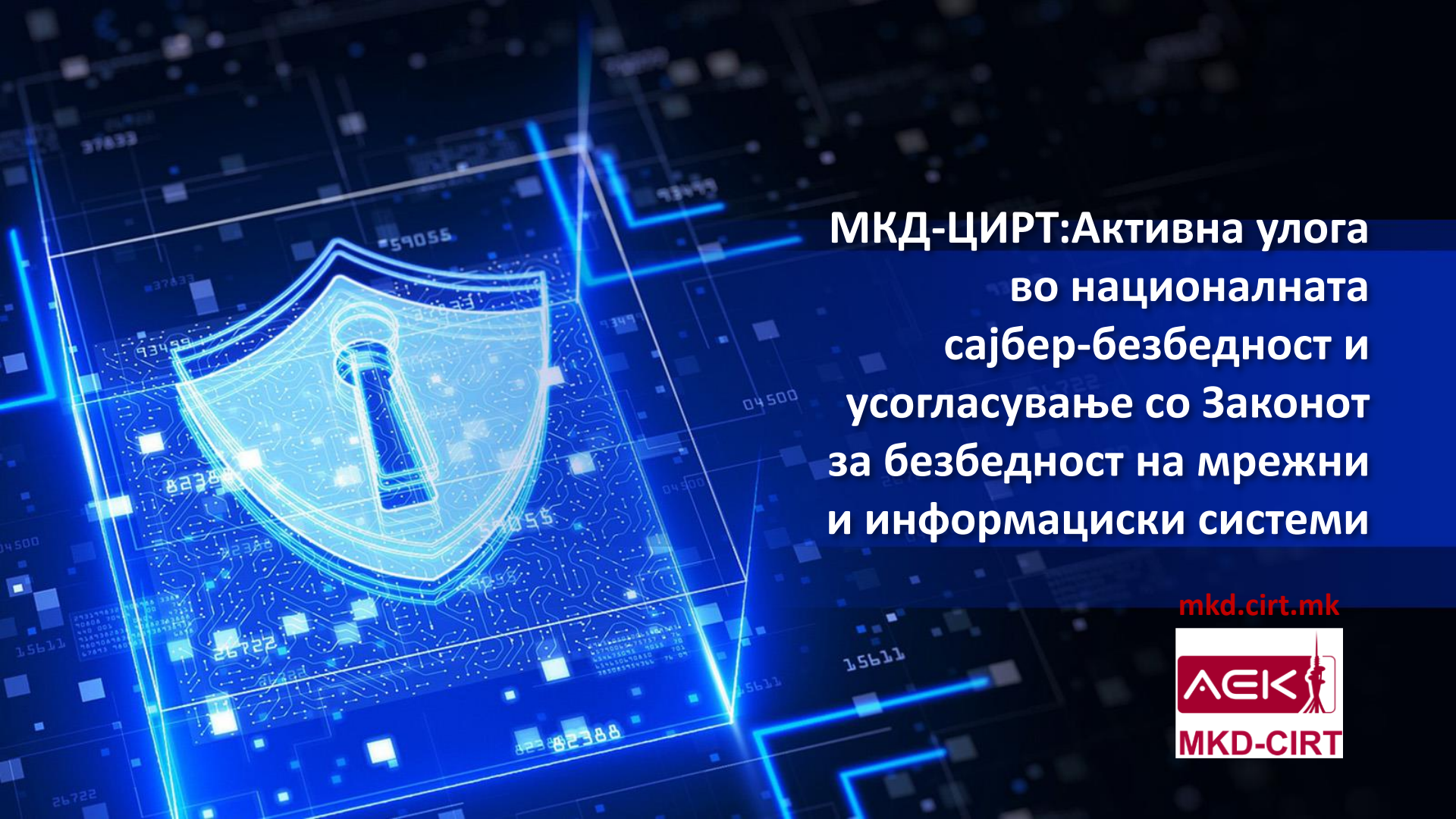

МКД-ЦИРТ:Активна улога
во националната
сајбер-безбедност и
усогласување со Законот
за безбедност на мрежни
и информациски системи
mkd.cirt.mk
MKD-CIRT

MKD-CIRT – Национален центар за одговор на компјутерски инциденти

Сектор во состав на **Агенцијата за електронски комуникации (АЕК)** одговорен за заштита, превенција и координација во областа на сајбер-безбедноста во РС Македонија

Главна улога:

- Превенција на сајбер-закани и зголемување на отпорноста на системите
- Координација и поддршка на институции и организации при справување со инциденти
- Размена на информации и соработка со меѓународни партнери
- Подигање на свеста на јавноста за безбедно користење на дигиталните услуги

Мисија и стратешки цели

Мисијата на MKD-CIRT е да обезбеди сигурен, доверлив и отпорен дигитален екосистем преку координирана заштита и стручна поддршка.

- Да координира и асистира на органите и институциите од јавниот и приватниот сектор во имплементацијата на проактивни услуги за намалување на ризикот од компјутерски безбедносни инциденти
- Да ја зголеми информираноста на граѓаните и организациите за ризиците од сајбер-закани
- Да обезбеди навремени совети, техничка помош и препораки при справувањена инциденти
- Да гради партнерства и воспостави национална и меѓународна мрежа за размена на информации
- 2016 - 2025 година -Изградена мрежа за размена на информации со над 150 организации од јавниот и приватниот сектор како и дел од операторите на критичните инфраструктури.

Цел: континуирано јакнење на капацитетите и развој на системи за рано предупредување и заштита.

Проактивни услуги и системи за надзор

Проактивните услуги кои ги обезбедва MKD-CIRT се насочени кон откривање и спречување на ризици пред да е предизвикана штета.

- **Објави и соопштенија (Announcements)** – навремени информации за нови ризици и закани
- **Следење на нови технологии (Technology Watch)** – идентификација на нови вектори на напад
- **Безбедносни ревизии и Пенетрациско тестирање (Security Audits & Pentesting)** – процена на нивото на заштита
- **Threat Intelligence Sharing** – споделување информации со конституенти и партнери
- **Услуга за Надзор над јавен веб** (.gov.mk домен).

Систем за сајбер-безбедносен надзор над мрежни инфраструктури –проактивно следење и рано откривање на сајбер-инциденти.

- Опфаќа над 30 организации со сензори за крајни точки
- Обезбедува автоматизирана анализа на мрежен сообраќај
- Овозможува рано предупредување и навремено известување до институциите
- Гарантира минимална инвазивност и максимална ефикасност при детекција
- Поддржува cloud-базирана заштита за јавни и владини субјекти

Цел: создавање интегриран национален систем за надзор, анализа и одговор на сајбер-ризици.

Реактивни услуги

MKD-CIRT обезбедува **реактивни услуги** со цел навремено откривање, анализа и одговор на инциденти кои можат да влијаат врз безбедноста на информациските системи.

- **Известувања и предупредувања (Alerts & Warnings)** – брза комуникација за откриени ризици и напади
- **Справување и координација при инциденти (Incident Response)** – техничка поддршка и координиран одговор
- **Управување со ранливости (Vulnerability Handling)** – анализа и координирано решавање на слабости
- **Анализа на закани и инциденти (Threat & Incident Analysis)** – истражување и препораки за превенција

Овозможуваат спречување на ширење на инцидентот, намалување на штетата, опоравување од настанатиот инцидент и споделување на искуството во насока на идна превенција

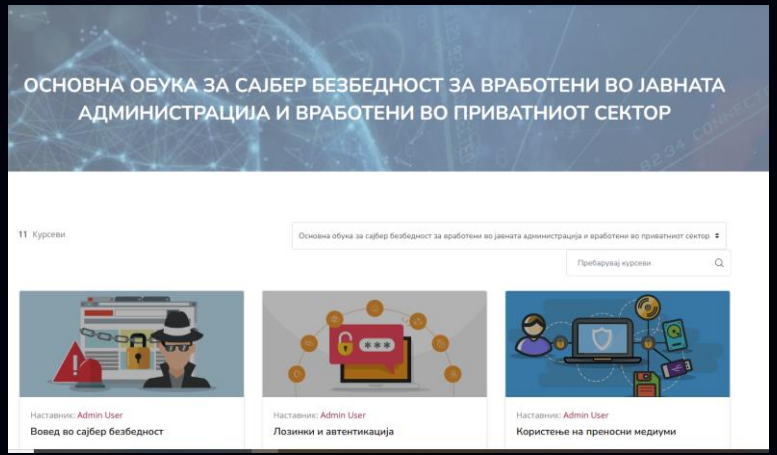
Управување со безбедносен квалитет, едукација и комуникација

MKD-CIRT спроведува активности, услуги и платформи насочени кон зголемување на безбедносниот капацитет на институциите, подигнување на свеста и воспоставување постојана комуникација со конституентите.

- **Проценка на безбедносен квалитет**
  Врши анализа на безбедносните поставки, препораки за подобрување и поддршка при спроведување технички и организациски мерки.

- **Развивање политики и стандарди**
  Подготовка на насоки и документи за унапредување на практиките за кибер-безбедноста кај јавни и приватни субјекти.

- **LMS платформа – lms.mkd-cirt.mk**
  Обезбедува онлајн обуки, курсеви и тестови за проценка на знаењето на вработените, со можност за добивање сертификат.



Управување со безбедносен квалитет, едукација и комуникација

CyberSafe.mk
Платформа за самооценување на организациите во однос на безбедносните политики и добивање бец „Сајбер одговорна организација“.

Aware.mkd-cirt.mk
Систем за предупредување и информирање за актуелни закани, препораки и совети за сајбер-безбедноста.

Cybermk.mk
Портал за информирање и споделување добри практики, вести и анализи во областа на сајбер-безбедноста.

Slack канал за комуникација со конституентите
Комуникациска платформа за брза размена на информации, координација и техничка поддршка помеѓу MKD-CIRT и институциите (критична инфраструктура, владини институции, регулатори и банкарскиот сектор)

Пријавување и управување со инциденти

MKD-CIRT овозможува безбеден и транспарентен процес за пријавување и управување со сајбер-инциденти.

Механизми за пријавување:

- **Анонимно пријавување** преку веб-страницата или е-пошта: info@mkd-cirt.mk
- **Пријави од конституенти** преку систем за пријавување и управување со инциденти
- **Пријави од други организации** со кои има воспоставено соработка и има доверба во точноста на доставените информации.

Анализа на ЗБМИС од перспектива на MKD-CIRT (АЕК)

MKD-CIRT е посебна организациона единица во рамките на Агенцијата за електронски комуникации (АЕК) и е надлежен орган за безбедност на МИС за дел од областите и субјектите (чл. 16) — со следниве клучни обврски:

- **Оперативно управување со инциденти и евиденции** Постапува по пријавени инциденти и да води евиденција за нив – (чл. 16 ст. 1 т. 4–5)
- **Предупредувања и информации**: издава предупредувања/соопштенија за ризици, закани, ранливости и инциденти – (чл. 16 ст. 1 т. 3)
- **Норми и упатства**: изготвува упатства, протоколи и технички правила за МИС за субјектите под негова надлежност (чл. 16 ст. 1 т. 2)
- **Координирано откривање на ранливости (CVD)**: е координатор и посредник во CVD процесот, вклучително и идентификација на засегнати субјекти,помош на пријавувачите; овозможува анонимно пријавување на ранливости – (чл. 24 ст. 1–4)
- Води **Национален регистар** на сајбер инциденти;
- **Стандардизација преку CSIRT мрежата**: утврдува/применува заеднички или стандардизирани практики, класификациски шеми и класификации за: процедури за справување со инциденти, управување со кризи и CVD (чл. 21 ст. 5)

- **Проактивно скенирање и анализа на ризик**: CSIRT тимовите (вклучително MKD-CIRT) можат да спроведуваат проактивно скенирање на јавно достапни системи на суштински/важни субјекти под нивна надлежност, и да приоретизираат задачи врз основа на анализа на ризик (чл. 22 ст. 2–3)

- **Меѓународна/ЕУ координација**: соработка со ENISA, EU-CyCLONe и други тела на ЕУ и НАТО преку CSIRT рамката (чл. 21 ст. 5–9)

Услуги и поддршка што MKD-CIRT треба да ги обезбеди

MKD-CIRT обезбедува интегриран систем на услуги кои го поддржуваат јавниот и приватниот сектор во зголемување на нивната отпорност на сајбер-инциденти.

Клучни услуги според Законот:

- **Инцидентен одговор и координација** за субјектите под негова надлежност – (чл. 20 ст. 1)
- **Евиденција и известување** за пријавени инциденти – (чл. 16 ст. 1 т. 5)
- **Проактивно скенирање** на јавно достапни системи и анализа на ризик – (чл. 22 ст. 2–3)
- **Предупредувања и соопштенија за ризици/закани/ранливости** (чл. 16 ст. 1 т. 3)
- **Соработка и стручна поддршка** кон други органи/ CSIRT тимови – (чл. 21 ст. 1–10)

MKD-CIRT исто така организира обуки, симулациски вежби и пенетрациски тестирања за подобра подготовка на институциите и операторите од суштинските и важните сектори во негова надлежност.

Субјекти под надлежност/надзор на MKD-CIRT

- Субјекти од чл. 4 ст. 1 т. 1), 2), 8) и ст. 2)–(3); експлицитно утврдено во чл. 20 ст. 1 (втора алинеја)
- **Субјекти без воспоставен сопствен секторски CSIRT**: доколку надлежните органи не воспостават CSIRT, надлежен станува MKD-CIRT (чл. 17 ст. 4)
- **Сите физички/правни лица како пријавувачи во CVD**: MKD-CIRT прима и обработува CVD пријави, вклучително анонимни (чл. 24 ст. 2–4)

Суштински и важни субјекти во рамки на MKD-CIRT надлежноста

MKD-CIRT е надлежен за сите суштински и важни субјекти кои управуваат со критична ИКТ-инфраструктура и чии услуги се од суштинско значење за функционирањето на државата, економијата и општеството.

Суштински субјекти:

- Енергетика
- Транспорт
- Банкарство и финансии
- Здравство
- Водоснабдување и управување со вода
- Дигитална инфраструктура

Важни субјекти:

- Поштенски и курирски услуги
- Управување со отпад
- Производство и дистрибуција на храна
- Одредени комуникациски услуги
- Јавна администрација и институции – Собрание, судови, државни органи и регулатори

Национална и меѓународна координација

MKD-CIRT е активен член на мрежата на CSIRT тимови и соработува со националните институции за навремена размена на информации и заеднички одговор на инциденти.

- Соработка со ENISA, EU-CyCLONe и NATO тела – (чл. 21 ст. 6–10)
- Учествува во меѓународни активности, обуки и координирани акции – (чл. 21 ст. 5–9)
- Поддржува размена на експертиза и добри практики во рамките на ЕУ механизмите – (чл. 15 ст. 2 т. 2–5)

Оваа координација е основа за интегрирана национална и европска отпорност на кибер-закани.

Рокови и применливост на новиот закон

Законот за безбедност на мрежни и информациски системи поставува јасни временски рокови за имплементација и усогласување.

- Подзаконски акти – во рок од 6 месеци од влегувањето во сила – (чл. 58 ст. 1)
- Детални листи на субјекти – во рок од 12 месеци – (чл. 58 ст. 2)
- Воспоставување на Мрежата и MKD-GOV-CSIRT – најдоцна за 12 месеци – (чл. 60 ст. 1)
- Примена на Законот – од 1 јануари 2026 година – (чл. 62)
- EU Одложена примена на одредени делови до членството во ЕУ – (чл. 61)

MKD-CIRT продолжува да функционира во рамките на АЕК, прилагодувајќи ја својата организација и процедури кон европските стандарди и практики.

Благодарам

mkd.cirt.mk

Biljana Jovanovska Baleski
National Center for Computer Incident Response | MKD-CIRT
Agency for Electronic Communications
biljana.jovanovska@aec.mk