Адреса
Кеј Димитар Влахов 21
1000 Скопје

Контакт
Тел.: 02 3091 232
Факс:02 3224 611
e-mail: info@mkd-cirt.mk

ГОДИШНА ПРОГРАМА ЗА РАБОТА НА НАЦИОНАЛНИОТ ЦЕНТАР ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ ЗА 2023 ГОДИНА

АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ
НАЦИОНАЛЕН ЦЕНТАР ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ MKD-CIRT

Скопје, октомври 2022

Содржина

1. Кратенки

сајбер простор, кибер простор	информациските системи и услуги директно или индиректно поврзани на Интернет, телекомуникациските и компјутерските мрежи, електронските комуникациски мрежи
CIRT	Computer (Cyber) Incident Response Team (тим за справување со компјутерски инциденти) Други кратенки со слично значење: CSIRT - Computer Security Incident Response Team CSRC - Computer Security Response Team CIRC - Computer Incident Response Center CERT - Computer Emergency Response Team IHT - Incident Handling Team IRC - Incident Response Center, IRT - Incident Response Team
MKD-CIRT	Национален центар за одговор на компјутерски инциденти https://mkd-cirt.mk
AEK	Агенција за Електронски Комуникации http://www.aec.mk
MARnet	Macedonian Academic Research Network (Македонска истражувачка Национална мрежа) http://marnet.mk
ITU	International Telecommunication Union http://www.itu.int/en/Pages/default.aspx
Национален/Владин CIRT	е тим кој и служи на државата и Владата на начин што и помага да ги заштити клучните/критичните информациски инфраструктури во државата. Националниот/Владин CIRT има клучна улога при координација на справувањето со инциденти кај засегнатите субјекти на национално ниво. Национален/Владин CIRT преставува официјална национална точка за контакт за размена на информации и соработка со Националните/Владини CIRT-ови од другите држави (според дефиниција на ENISA)
ENISA	European Union Agency for Network and Information Security https://www.enisa.europa.eu/

FIRST	Forum for Incident Response and Security Teams https://www.first.org/
TF-CSIRT	Trusted Introducer https://www.trusted-introducer.org/
CERT-EU	Computer Emergency Response Team for EU institutions https://cert.europa.eu/cert/plainedition/en/cert_about.html
MATRIX	Точка за размена на интернет сообраќај при MARnet
МИОА	Министерство за информатичко општество и администрација на РСМ
МВР	Министерство за внатрешни работи на РСМ
ЦУК	Центар за управување со кризи на РСМ
МОН	Министерство за образование и наука на РСМ
МТСП	Министерство за труд и социјална политика на РСМ

2. Правен основ за донесување на програмата

Врз основа на член 26-а став 2 и 3 од Законот за електронските комуникации („Службен весник на Република Македонија“ бр. 39/14, 188/14, 44/15, 193/15, 11/18 и 21/18 и „Службен весник на Република Северна Македонија“ бр.98/19 и 153/19), Директорот на Агенцијата за електронски комуникации во соработка со министерот надлежен за работите од областа на електронските комуникации донесува Годишна програма за работењето на националниот центар за одговор на компјутерски инциденти формиран како посебна организациона единица во состав на Агенцијата за електронски комуникации и истата ја доставува на усвојување од страна на Владата на Република Северна Македонија.

3. Вовед

Сајбер безбедноста има се поголемо значење за организации од сите големини низ секоја индустрија и во секој сектор. Сајбер нападите продолжуваат да се зголемуваат.

Не треба да изненадува што фишингот и понатаму е на врвот на трендови во компјутерската безбедност, и се чини дека нема да се намали во скоро време. Денес фишингот не е само за е-пошта - иако е-поштата е сè уште најпопуларен вектор за напад. Интернет-криминалците исто така користат и други вектори за напади за да ги измамат корисниците со цел откривање на лични податоци, кражби, уцени и измами. Сè повеќе, фишингот вклучува напади со СМС-пораки.

Дополнителни трендови за 2022-23 година вклучуваат таргетирање на владиниот, јавниот и критичните сектори со рансомвер и DDoS напади, како и зголемен интерес и инвестиции во користење на вештачката интелигенција и машинското учење како двигатели на развој на сајбер одбраната, но и сајбер нападите.

Годишната програма за работа на Националниот центар за одговор на компјутерски инциденти има за цел преку реализација на активностите за исполнување на зацртаните цели, да се зголеми отпорноста на сајбер-напади за јавниот и владиниот сектор во државата, на операторите на критични информациски системи, како и континуирано да се подобрува на граѓаните и приватниот сектор за сајбер / кибер безбедноста.

4. ЗА MKD-CIRT

4.1. За центарот

Со измените на Законот за електронските комуникации (Службен весник на Република Македонија број 188/2014), согласно член 26-а во состав на Агенцијата за електронски комуникации се формира посебна организациона единица - Национален центар за одговор на компјутерски инциденти MKD-CIRT, како Национален CSIRT на Република Северна Македонија, кој претставува официјална национална точка за контакт и координација во справувањето со безбедносните инциденти кај мрежите и информациските системи и кој идентификува и обезбедува одговор на безбедносни инциденти и ризици.

МИСИЈА

Националниот центар за одговор на компјутерски инциденти ја има следната мисија:

a) да координира и да помага/асистира на органите и институциите од јавниот сектор во имплементацијата на проактивни услуги за намалување на ризикот од компјутерски безбедносни инциденти, како и при справувањето со инцидентите кога истите ќе настанат ,
b) да спроведува активности за едуцирање и подигање на свесноста кај граѓаните за негативните ефекти на сајбер-заканите и компјутерскиот криминал, и
c) навремено да обезбедува совети за сите негови конституенти.

КОНСТИТУЕНТИ

Во реализацијата на програмата за работа за 2023 година MKD-CIRT ќе вклучи организации од следните сектори: финансии, комуникации, енергетика, водоснабдување, итни услуги, храна, јавна безбедност, здравство и услуги на е-влада. Во 2023 година ќе се продолжи со активностите за идентификација на операторите на критичните инфраструктури во државата, согласно националната стратегија за сајбер-безбедност, позитивната национална легислатива и најдобрите практики од Европската Унија и НАТО. MKD-CIRT ќе продолжи со размена на информации со постојните и нови организации како конституенти на MKD-CIRT, како и потпишување на поодделни Договори за соработка и одговорно откривање на информации. MKD-CIRT во периодот 2017 - 2022 година изгради мрежа за размена на информации со над 90 организации од јавниот и приватниот сектор како и дел од операторите на критичните инфраструктури. Цел во 2023 година ќе биде вклучување на операторите од критичните инфраструктури согласно класификацијата на критични сектори во европската директива за мрежна и информациска безбедност и националната легислатива.

4.2. Цели и задачи на MKD-CIRT

Ц 1	**Да обезбеди клучна улога при координација на справувањето со инциденти кај засегнатите субјекти на национално ниво.**
Ц 2	**Да обезбеди одговор за справување со компјутерски инциденти, преку давање на неопходни услуги кон неговиот конституент/корисник, со што неговиот конституент/корисник ќе може ефикасно да се справи со инцидентите.**
Ц 3	**Континуирано да врши мониторингот за ризици, да добива информации за компјутерските закани и инциденти (по автоматски пат или од трети страни) и постојано да располага со показатели за малициозниот сообраќај што доаѓа или излегува од државата.**
Ц 4	**Преставува официјална национална точка за контакт и размена на информации (извештаи за инциденти, ранливост итн.) за внатре во рамките на државата како и за надвор од неа со Националните/Владини CIRT-ови од државите во регионот и пошироко.**
Ц 5	**Навремено да ги информира и известува конституентите. Да им обезбедува на конституентите безбедносни совети, информации за рано предупредување и да делува како централна точка за прашањата од областа на сајбер безбедноста.**
Ц 6	**Целосно да соработува и разменува информации со институциите од државата надлежни за спроведување на законите, а особено со оние од областа на сајбер-криминалот, како и соодветно да ги адресира правните прашања кои можат да се појават за време на инцидент.**
Ц 7	**Континуирано да разменува информации, знаење и искуство со конституентите, да утврдува безбедносни најдобри практики/водичи и истите да ги објавува, како и континуирано да обезбедува едукација и обуки за конституентите и за самите вработени во центарот.**
Ц 8	**Да обезбедува помош во процесот на воспоставување на Интерни центри за одговор на компјутерски инциденти на големите организации кои управуваат со клучни/критични информациски инфраструктури (јавни и приватни) во државата.**
Ц 9	**Континуирано да ја подига свесноста кај граѓаните за негативните ефекти на сајбер заканите и компјутерскиот криминал.**

5. Услуги на MKD-CIRT

5.1. Типови на услуги

Услугите што MKD-CIRT ќе ги понуди во 2023 година на своите конституенти, граѓаните, јавниот и приватниот сектор се поделени во неколку групи, и тоа реактивни, проактивни и услуги за управување со квалитетот на безбедноста - Security Quality Management.

РЕАКТИВНИ УСЛУГИ

Реактивните услуги вклучуваат известувања од страна на конституент по настанат инцидент или други настани во врска со закани и напади како на пример: компромитиран уред, штетен софтвер/малвер, ранливост или друг тип на слични инциденти. По пријава на инцидент MKD-CIRT постапува со мерки кои имаат за цел спречување на ширење на инцидентот, намалување на штетата, опоравување од настанатиот инцидент и споделување на искуството во насока на идна превенција.

У1. Известувања и предупредувања (Alerts & Warnings)
У2. Справување со инцидент, координација и одговор на инцидент (Incident response and handling)
У3. Справување со ранливост, координација и одговор на ранливости (Vulnerability handling)
У4. Анализа на закани и ранливости

ПРОАКТИВНИ УСЛУГИ

Проактивните услуги имаат за цел детекција и превенција на нападите пред истите да се случат. Во оваа категорија на услуги, информациите и знаењето со кои располага тимот на MKD-CIRT се дистрибуира до конституентите и соработниците со цел тие да се ги заштитат своите средства и да не станат цел на напади. Проактивните услуги кои MKD-CIRT ќе ги понуди во 2022 година се:

У5. Објави / Announcements
У6. Следење на нови технологии / Technology watch
У7. Безбедносни ревизии / Pentest
У8. Споделување на информации за закани / Threats intelligence sharing

SECURITY QUALITY MANAGEMENT

Овие услуги имаат за цел промена и подобрување на постојни и етаблирани услуги кои се независни од управување со инциденти и најчесто ги реализираат други оддели кај конституентите (ИТ, ревизија и сл.) Информациите и знаењето со кое располага тимот на MKD-CIRT ќе помага во подобрување на безбедносните аспекти кај услугите кои ги реализираат конституентите. Цел е да се идентификуваат ризиците, заканите и слабостите на иформациските системи кај конституентите. Овие услуги генерално се проактивни, но допринесуваат индиректно за намалување на бројот на инциденти. Услуги што MKD-CIRT ќе ги реализира во делот за управување со квалитетот на безбедноста во 2023 година се:

- анализа на ризик
- деловен континуитет и Disaster Recovery планирање
- безбедносни консултации

5.2. Достапност на услугите

Согласно усвоените препораки во извештајот на ITU-IMPACT, услугите кои MKD-CIRT ќе ги пружа на конституентите и граѓаните на Република Северна Македонија се поделени во три групи: основни, подобрени и напредни услуги. И во 2023 година предуслов за успешно пружање на овие реактивни и проактивни услуги останува квалитетно и целосно екипирање на тимот на MKD-CIRT. Заради недостаток на квалитетен стручен кадар (доекипирање) услугите од групата „напредни услуги“ се одложуваат за период 2023-24 година.

MKD-CIRT дополнително ги прилагодува услугите согласно Националната стратегија за сајбер-безбедност и Акцискиот план. Во моментот на создавање на овој документ сеуште важечка е Национална стратегија за сајбер безбедност со Акциски план 2018-2022. Се очекува Владата на РСМ да усвои втора Национална стратегија за сајбер безбедност до крај на 2022 година, по што може да следат измени и усогласувања на активностите, услугите и проектите на MKD-CIRT во овој документ.

I	**Основни услуги (Basic services)**

1	Известувања и предупредувања	Откривање на детали за тековните закани и чекори кои можат да се преземат за заштита од овие закани. Вклучува известување или предупредување за новооткриената информација за сајбер закани и слабости до конституентите со препорачан тек на акции и насоки за тоа како да се заштити системот. Известувањата може да се превентивни, предупредувачки, советодавни, и насочувачки.
2	Далечински одговор на инцидент	Обезбедување на техничка помош за справување со безбедносните инциденти кога ќе се појават, со цел ублажување на штетата и опоравување од инцидентот. Советите и техничката помош вообичаено ќе се обезбедуваат преку телефон или e-mail базирана комуникација
3	Одговор на инцидент на лице место	Обезбедување на техничка поддршка и совети за справување со безбедносните инциденти кога ќе се појават на лице место кај конституентот, со цел ублажување на штетата и опоравување од инцидентот. Оваа услуга вообичаено е поврзана и се реализира при инциденти од критично ниво. Заради потреба од доекипирање на центарот оваа услуга се одложува за период 2023-24 година.
4	Одговор на ранливост	Оценување на соодветни мерки потребни за да се одговори на новооткриени слабости; да се оцени нивната сериозност и влијание, да се одлучи дали да издадат предупредувања за нив или да се потврдат или понатаму да се испита нивната тежина / влијание. Генерално, овој пристап се однесува на информации за ранливости кои се веќе јавно познати.
5	Основна свест, едукација и обука	Спроведување на програми за подигнување на јавната свест. Спроведување на основни обуки за одговор на компјутерски инциденти и основни сајбер безбедносни најдобри практики.

II	**Подобрени услуги (Enhanced services)**

6	Координација на одговор на инцидент	Дејствување како координативна точка на национално или регионално ниво помеѓу страните засегнати од безбедносниот инцидент. За да може да ја обезбеди оваа услуга, MKD-CIRT мора да воспостави и одржува доверлива

		комуникација со различни страни и агенции на национално, регионално и глобално ниво.
7	Напредна свест, едукација и обука	Спроведување на програми за подигање на јавната свест како на пр. конференции на национално или регионално ниво. Спроведување на напредни обуки за одговор на компјутерски инциденти и напредни сајбер безбедносни најдобри практики.
8	Координација на одговор на ранливост	Координација на одговорно објавување на информации во врска со софтверски/хардверски ранливост во соодветен временски период. Времето на објава се одредува на тој начин за да се минимизираат негативните последици од предвремено откривање, преку обезбедување на доволно време за добавувачот да развие и објави закрпа и тоа време да се совпадне со известувањето.
9	Анализа на закани и ранливости	Анализата на компјутерски и мрежни закани и ранливости со цел да се одреди нивното можно/потенцијално влијание и како најдобро истите да се ублажат; Идентификација на новите трендови или промени во начинот на работење на напаѓачот; или советување во врска со општите трендови во сајбер безбедноста.

III Напредни услуги (Advanced services)

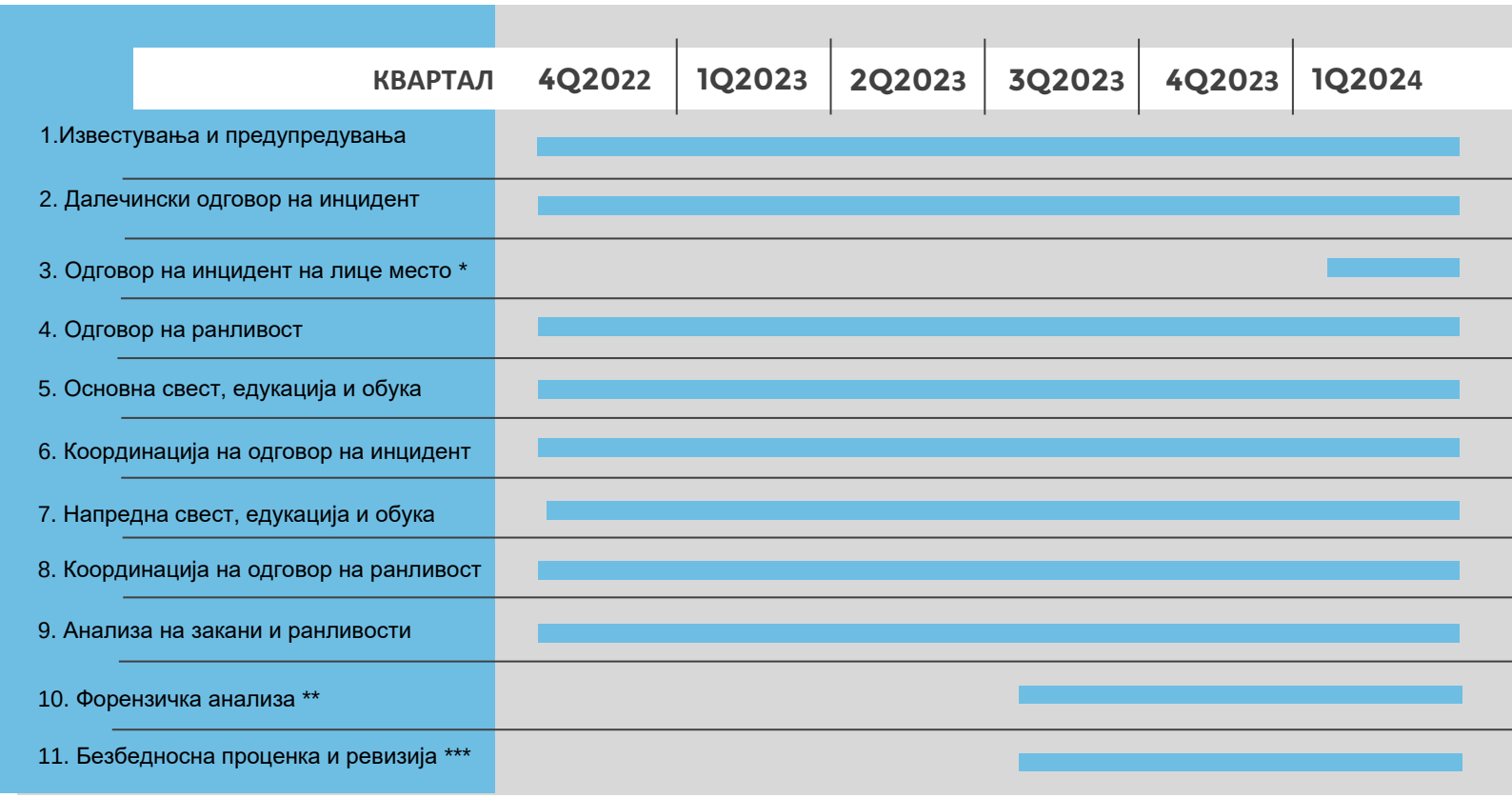
10	Форензичка анализа	Спроведување на дигитални форензички анализи на дигитални докази и артефакти во согласност со законите во Република Северна Македонија. Тоа е реактивен услуга со која членовите на тимот на MKD-CIRT ќе реагираат и одговорат на инцидентот преку испитување и утврдување на штета, оправување и евентуално идентификација на сторителот.
11	Безбедносна проценка и ревизија	Консултантски услуги за да обезбеди извештај за процена на безбедноста на информатичките системи / мрежи на Конституентот; истакнување на сите слабости и предлагање на методи за да се подобри безбедноста. Вид на услуги: - анализа на ризик - деловен континуитет и Disaster Recovery планирање - безбедносни консултации

За реализација на услугите на MKD-CIRT неопходно е:

- екипирање на тимот со квалитетен кадар,
- континуирана едукација на членовите на тимот,
- имплементација и користење на соодветна опрема за оцена на ранливост на системите и мрежите кај конституентите,
- Имплементација на опрема за форензичка анализа по настанат инцидент кај конституент и анализа на малвер/штетен софтвер, како и
- обука на вработените во тимот за користење на опремата.

Услугите на MKD-CIRT кои се однесуваат на справување со пријавен инцидент кај конституент може да побаруваат потпишување на соодветни договори со кои ќе се дефинира опсегот на системите и мрежите кои ќе бидат предмет на анализа и истражување по пријавениот инцидент како и за предложени и прифатени мерки за ублажување на влијанието на инцидентот и оправување на мрежите и системите на конституентот.

Период на достапност на услугите во 2023 година по квартали



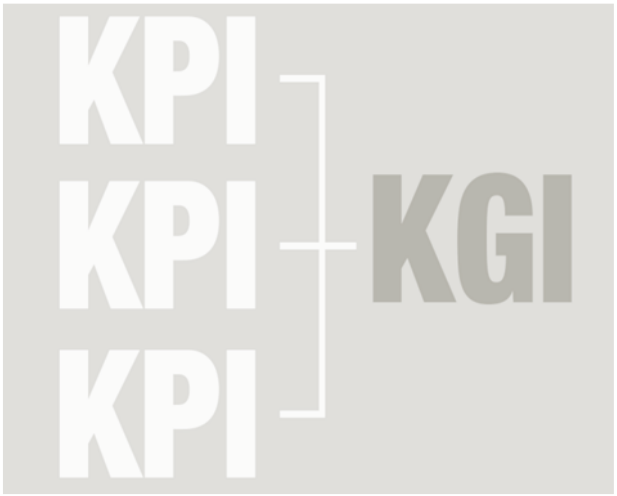
*пренесено од 2022 во 2023/24, заради потребата за екипирање на тимот и вработување на најмалку 3 нови вработени што не е реализирано во 2022 година;

**пренесено од 2022 во 2023 година, бидејќи опремата за форензичка анализа е инсталирана и за нејзино користење неопходно е доекипирање преку дополнително вработување на нови лица, а услугата ќе биде достапна по екипирање на тимот со нови вработени;

*** Услугата за Безбедносна проценка и ревизија ќе отпочне да се пружа по екипирање на центарот

Заради потребата од доекипирање на тимот на MKD-CIRT преку нови вработувања и потребата од дополнителна едукација на вработените во делот на дигитална форензика и процена на ранливости, услугите број 3, 10 и 11 се одложени за 2023/24 година, и реализацијата на истите ќе зависат од зголемување на бројот на членовите во тимот на MKD-CIRT и нивната едукација во 2023/24 година.

6. Акциски план



Акцискиот план е прикажан во облик на активности кои MKD-CIRT ќе ги реализира во текот на 2023 година за исполнување на претходно наведените цели.
Во продолжение е даден табеларен приказ на секоја од целите дополнета со информации за Клучни индикатори за исполнување на цел (KGI - Key Goal Indicator). Секој KGI е пропратен со еден или повеќе Клучен Показател на успешност (KPI - Key Performance Indicator). Активностите се дополнети и со референца кон Акцискиот план за Стратегија за сајбер безбедност (АПССБ). Актуелната стратегија е за период 2018-2022 година и овој документ е изработен пред донесување на национална стратегија за сајбер-безбедност за период од 2023.

(Ц1) ОБЕЗБЕДИ КЛУЧНА УЛОГА ПРИ КООРДИНАЦИЈА НА СПРАВУВАЊЕТО СО ИНЦИДЕНТИ КАЈ ЗАСЕГНАТИТЕ СУБЈЕКТИ НА НАЦИОНАЛНО НИВО.
KGI 1.1 Развиена мрежа за навремена координација на одговор по инциденти и размена на информации
KPI 1.1.1 Дефинирани оператори од критични сектори со кои MKD-CIRT ќе соработува
KGI 1.2 Национална рамка за информациска безбедност
KPI 1.2.1 Учество на MKD-CIRT и АЕК во развој и имплементација на стратегија, законски и подзаконски решенија

KGI 1.1. Мрежа за размена на информации

При пријава или идентификација на компјутерски инцидент, Националниот центар за одговор на компјутерски инциденти како национален CSIRT ќе обезбеди клучна улога при координирање на активностите кои ќе бидат потребни да се спроведат за справување со компјутерскиот инцидент. Координацијата се однесува на вклучување и известување на засегнати субјекти на национално ниво, за решавање и надминување на пријавениот компјутерски безбедносен инцидент. Овие активности се во врска исполнување на обврската согласно член 26-а од Законот за електорнските комуникации, како и со задача 5.1.2, 5.1.3 и 5.1.4 од АПССБ.

За исполнување на оваа цел во 2023 година ќе се реализираат следните активности:

- навремено ќе се ажурира регистар на контакти со конституенти за справување со кризна состојба и инциденти;

- ќе се обезбеди високо ниво на достапност на различни доверливи канали за комуникација со соодветните субјекти на национално ниво;

• ќе се подготвуваат соодветни упатства и процедури за надминување на стандардни и познати компјутерски инциденти и безбедносни закани;

Дополнително не постои дефиниција за критични сектори и оператори на критична инфраструктура. Во насока на дефинирање на критични сектори, во 2023 година MKD-CIRT ќе продолжи со нивна идентификација согласно Националната стратегија за сајбер-безбедност, важечката легислатива во Република Северна Македонија и согласно Европската NIS директива.

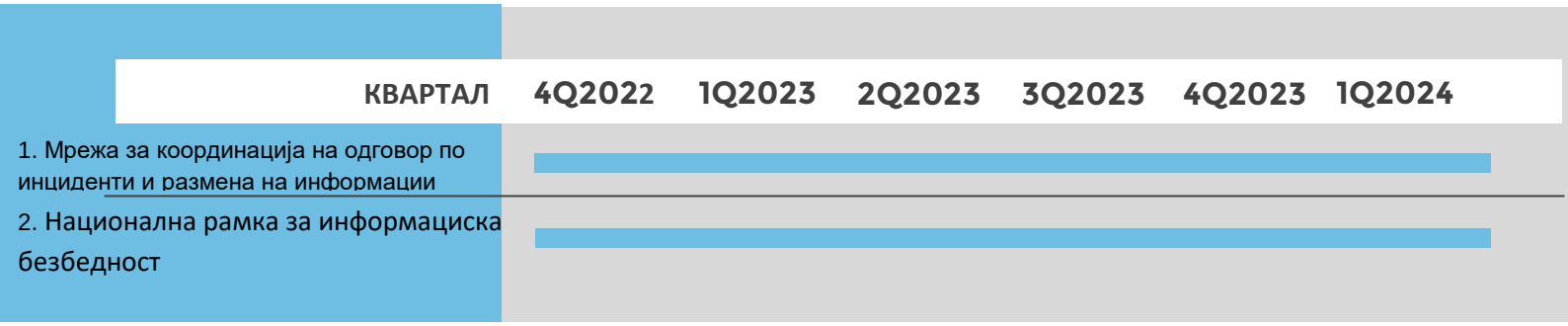
• ревизија на постојни и изработка на нови упатства, правилници и други подзаконски акти за размена и објава на информации по инциденти, закани и ризици;

Оваа активност е согласно точка 1.3.1 „ Дефинирање на листа на КИИ и ВИС врз основа на Студија за дефинирање и идентификација на КИИ и ВИС “од АПССБ.

KGI 1.2. Национална рамка за информациска безбедност

Како член во работната група за реализација на АПССБ, во насока на дефинирање на обврските и делокругот на работење, Агенцијата и MKD-CIRT и понатаму ќе дава конструктивни мислења по документите од областа на информациската безбедност. Во текот на 2023 година MKD-CIRT ќе учествува согласно какапцитетите на тимот во изработка на анализи, препораки и предлози за транспонирање на европската директива за мрежна и информациска безбедност- The directive on security and information systems (NIS Directive) 2016/1148, како и имплементација на предлозите за усогласување на активностите за национални CSIRT тимови објавена од страна на ENISA - NIS Directive and national CSIRTs, објавено на 26.02.2016 година.

Период за реализација



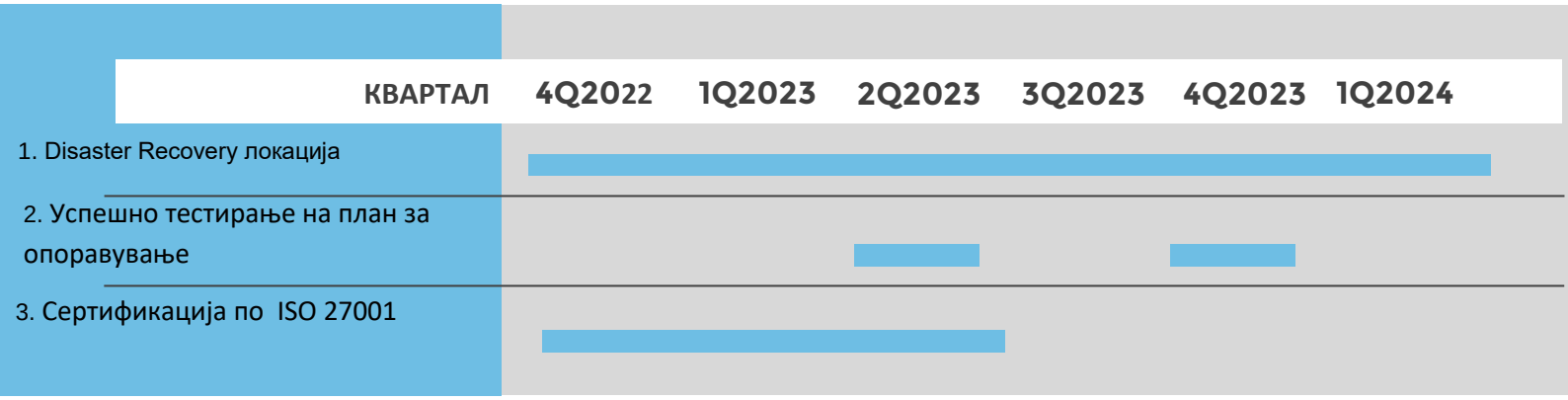
(Ц2) ОБЕЗБЕДУВАЊЕ НА ОДГОВОР ЗА СПРАВУВАЊЕ СО КОМПЈУТЕРСКИ ИНЦИДЕНТИ, ПРЕКУ ДАВАЊЕ НА НЕОПХОДНИ УСЛУГИ КОН НЕГОВИОТ КОНСТИТУЕНТ/КОРИСНИК, СО ШТО НЕГОВИОТ КОНСТИТУЕНТ/КОРИСНИК ЌЕ МОЖЕ ЕФИКАСНО ДА СЕ СПРАВИ СО ИНЦИДЕНТИТЕ.
KGI 2.1 Навремен, стручен и корисен одговор до конституент по пријавен инцидент
KPI 2.1.1 Време за одговор и решавање по пријавен инцидент, број и тип на инциденти
KPI 2.1.2 Високи нивоа на достапност и доверливост на каналите за пријава на инциденти и комуникација

KGI 2.2 Едуциран и стручен кадар – членови на тимот на MKD-CIRT KPI 2.2.1 Реализирани обуки и Сертификација на членовите на тимот како потврда на стекнатите вештини

KGI 2.1. Достапноста на услугите на MKD-CIRT во 2022 година предлагаме да се подобри преку:

- Користење и периодични проверки на опрема за висока достапност на услугите преку воспоставена локација за Disaster Recovery и тестирање на соодветен план за оporавување, согласно барањата од Annex I од Directive (EU) 2016/1148 - The Directive on security of network and information systems (NIS Directive)
- Сертификација на MKD-CIRT по ISO/IEC 27001 стандардот за Information Security Management System (активност почната преку реализација на консултантски услуги за имплементација на овој стандард во 2020 и се очекува да заврши во првата половина на 2023 година зависно од обезбедени финансиски средства).

Период за реализација



Финансиски трошоци

1. Сертификација на MKD-CIRT согласно ISO 27001 (дел од проект на Агенцијата за 2022 за сертификација по овој стандард– нема посебен буџет за MKD-CIRT, ќе се реализира согласно достапни средства на Агенцијата)	/
2. Адаптивно и Превентивно одржување на ИКТ опремата на MKD-CIRT	11.700.000,00 ден.

Оваа активност е предуслов за реализација на точка 1.1.2 „ Проширување на бројот на понудени услуги согласно NIS директивата “од АПССБ. Истата е согласно Анекс 1 од NIS директивата на ЕУ.

KGI 2.2. Јакнење на капацитети на тимот

За реализација на услугите на MKD-CIRT неопходно е:

- екипирање на тимот со квалитетен кадар,
- континуирана едукација на членовите на тимот

Во период 2016 - 2022 година MKD-CIRT ги реализираше активностите со два члена кои повремено извршуваат и активности за Служба за информатички технологии во Агенцијата.

Во 2023 година неопходна е дополнително вработување на кадар (3 нови вработени) согласно важечката систематизација на Агенцијата за електронски комуникации, како и едукација на вработените со реализација на следните обуки со прикажани финансиски трошоци:

- TERENA/GEANT TRANSITS 1/2, Задолжителна обука за нови вработени во MKD-CIRT. Обуките ќе имаат за цел тренинг за процесот за справување со инциденти.
- Сертифицирани обуки организирани од SANS и други докажани меѓународни провајдери на теми:
  - Детекција на упад
  - Напредна компјутерска форензичка анализа и одговор на инциденти
  - Тестирање на мрежи и системи за ранливости и етичко хакерство
  - Хакерски техники, експлоатирање и управување со инциденти

Период за реализација

КВАРТАЛ	4Q2022	1Q2023	2Q2023	3Q2023	4Q2023	1Q2024
1. Обуки и сертификација на вработените во Националниот центар MKD-CIRT						

Финансиски трошоци

1. Обуки за вработени и конституенти	/

Реализацијата на оваа активност е условена со барање помош од меѓународна организации и донации, и од буџет на Агенцијата за 2023 година наменет за обуки. Оваа активност е во врска со точка 1.1.1 „ Зголемување на број на вработени во центарот со доекипирање, пополнување на работни позиции и контунирана едукација на кадарот во делот на справување со инциденти, анализа на малвер, безбедносни проверки и форензика “од АПССБ. Истата е согласно Анекс 1 од NIS директивата на ЕУ.

(Ц3) КОНТИНУИРАНО ДА ВРШИ МОНИТОРИНГОТ ЗА РИЗИЦИ, ДА ДОБИВА ИНФОРМАЦИИ ЗА КОМПЈУТЕРСКИТЕ ЗАКАНИ И ИНЦИДЕНТИ (ПО АВТОМАТСКИ ПАТ ИЛИ ОД ТРЕТИ СТРАНИ) И ПОСТОЈАНО ДА РАСПОЛАГА СО ПОКАЗАТЕЛИ ЗА МАЛИЦИОЗНИОТ СООБРАЌАЈ ШТО ДОАЃА ИЛИ ИЗЛЕГУВА ОД ДРЖАВАТА

KGI 3.1. Систем за собирање, анализа и дистибуција на информации за ризици, закани, ранливости и инциденти (Threats Intelligence / Сајбер ризици, закани и ранливости на национално ниво)

KPI 3.1.1 Систем за собирање, анализа и дистибуција на информации за ризици, закани, ранливости и инциденти (Threats Intelligence System)

KPI 3.1.2 Поврзување на TIS со постојни системи за пријава на инциденти и MISP

KPI 3.1.3 Автоматизирано алармирање и препраќање на надворешни пријави до засегнати конституенти и оператори – даватели на услуга за интернет

KGI 3.2 Процена на ризици на државно ниво

KPI 3.2.1 Учество на MKD-CIRT во работната група за АПССБ за изработка на Методологија за процена на ризиците на национално ниво со нивоа на закани

KPI 3.2.2 Систем за автоматизирана процена на веб-ранливости

KPI 3.2.3 Систем за сајбер-безбедносен надзор над мрежни инфраструктури

KPI 3.2.4 Фишинг кампањи и едукација

KGI 3.3 Извештајност

KPI 3.3.1 Објава на извештаи и информации за закани, ранливости и инциденти на веб-страницата https://mkd-cirt.mk

KGI 3.4. Систем за управување со компјутерски инциденти и сајбер безбедностни настани и информации

KGI 3.1. Систем за собирање, анализа и дистибуција на информации за ризици, закани, ранливости и инциденти (Threats Intelligence / Сајбер ризици, закани и ранливости на национално ниво)

Системот во облик на група услуги за управување со сајбер ризици, закани и ранливости на национално ниво треба да овозможи појасен преглед на актуелните закани и ризици на национално, секторско и организациско ниво. Дополнително овој систем е поврзан со систем на MKD-CIRT за пријава на инциденти и во 2023 се планира интеграција со MISP системот. Овој систем треба да овозможи користење на комерцијални извори на информации. Станува збор за лиценцирани решенија со годишни трошоци за користење на услугите, со вклучен моментален преглед и состојба на национално, секторско и организациско ниво.

Оваа активност е согласно 1.4.1. „ Следење на најновите закани врз сајбер безбедност “ и 1.4.3 „ Континуирано унапредување на технолошките и организациските мерки за ефикасно справување со сајбер заканите. “ од АПССБ.

KGI 3.2. Процена на ризици на државно ниво

Во 2019 година MKD-CIRT формално беше вклучен во работата на работната група за реализација на акцискиот план за стратегијата за сајбер-безбедност. MKD-CIRT како дел од работната група ќе учествува во изработка на Методологија за процена на ризиците на национално ниво.

Во 2023 година, MKD-CIRT ќе понуди услуга на конституентите за процена на ранливости во мрежите и системите кај конституентите и во соработка со Министерството за информатичко општество и администрација ќе ги дефинира методологијата за проценатa и условите за користење на оваа услуга. За успешно спроведување на оваа услуга предуслов е доекипирање на тимот на MKD-CIRT.

Во 2023 година MKD-CIRT ќе продолжи со услуга за Надзор над јавен веб на јавниот веб (.gov.mk домен). Цел на услугата е да се има увид во достапноста на веб-страниците поставени на домените кои се сопственост на владиниот и јавниот сектор и прибирање на информации за достапност и резултати од безбедносно скенирање. Системот ќе овозможи и активно скенирање и навремено известување на организацијата-сопственик на доменот за откриените слабости и ранливости.

Во 2023 година MKD-CIRT ќе продолжи со користење и развој на систем за автоматизиран увид во тип на надворешен мрежен сообраќај кај дел од конституентите од јавниот и владиниот сектор (до 10 дополнителни организации/оддалечени точки со дополнителни крајни корисници) - „ Систем за сајбер-безбедносен надзор над мрежни инфраструктури “. Оваа услуга има за цел преку анализа на карактеристиките на надворешниот сообраќај на конституентот, да се добијат информации за закани, ризици и рано предупредување на нови напади, со испраќање на информации и до организацијата кои треба да ги имплементира. Секоја од организациите вклучени во системот има детален увид во своите активности и навремено алармирање. Цел на системот е преку анализа на облик на сообраќај, минимална инвазивност, да се овозможи рано предупредување на конституенти за напади и ранливости, со крајна цел намалување на ризиците. Дополнително организациите вклучени во надзорот ќе имаат cloud-базирана заштита за работата на вработените/уредите преку cloud-base заштита и поставени сензори за крајни корисници/уреди. Истовремено АЕК и MKD-CIRT преку овој систем и сензори ќе имаат увид и информации за напади и ризици и малициозна комуникација, што е во насока на исполнување на обврските согласно член 166-а од Законот за електронските комуникации.

Во 2023 година MKD-CIRT предлага нова услуга за тестирање на фишинг напади и кампањи, што би ја понудиле на конституентите. На тој начин АЕК и MKD-CIRT како и организациите ќе имаат увид во моментално ниво на едукација кај вработените за преознавање на фишинг напади и насоки и материјали за дополнителна едукација. Оваа активност е согласно точка 1.1.2, 1.4.1 и 1.4.3 од АПССБ.

Фишинг капмањи и едукација – цел е да се постави и овозможи нова услуга за тестирање на ниво на знаење кај граѓани и вработени за препознавање на фишинг пораки и насочување кон едукативни содржини за подобрување.

KGI 3.3. Извештајност

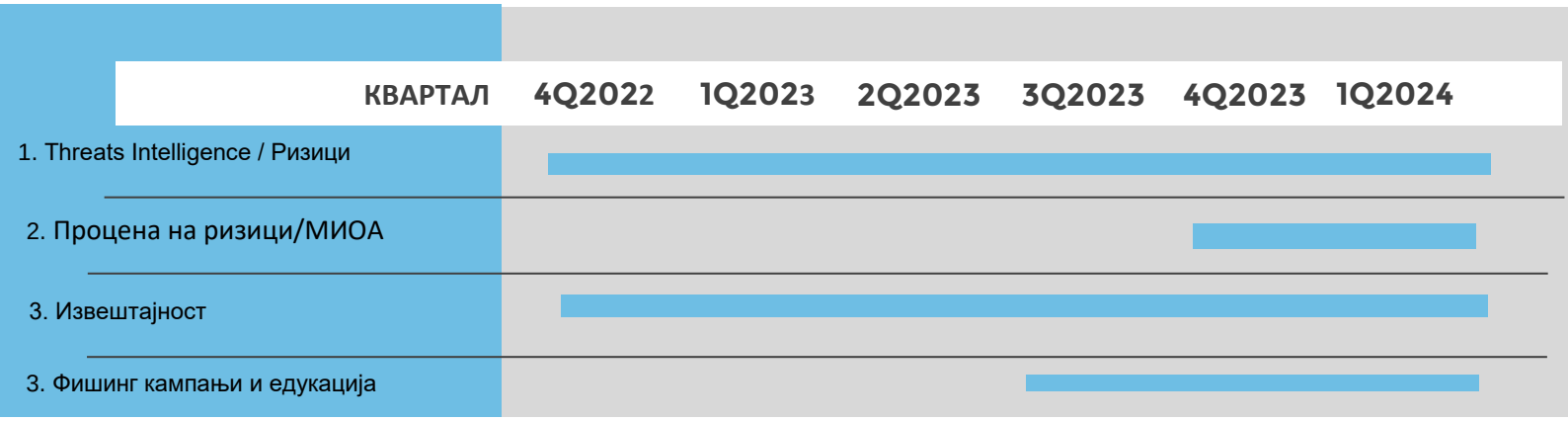
Во 2023 година MKD-CIRT ќе објавува извештаи и информации за закани, инциденти, штетен софтвер и совети.

Оваа активност е согласно точка 1.1.2, 1.4.1. 1.4.4 и 1.4.3 од АПССБ.

KGI 3.4. Систем за управување со компјутерски инциденти и сајбер безбедностни настани и информации

Во 2023 година се планира продолжување и понатамошна консолидација на системите и алатките на MKD-CIRT за пријава, обработка и постапување по инциденти со дополнителни услуги за експертка помош во анализа на пријави и постапување по инциденти.Со оваа активност ќе се заменат постари системи со понови и модерни софтверски решенија. Дополнително се планира продолжување на лиценцирање за постојни решение, како Решение за анализа на злонамерни содржини / малвер и негова интеграција со системите на MKD-CIRT.

Период за реализација



Финансиски трошоци

1. Threats Intelligence / управување со сајбер ризици, закани и ранливости на национално ниво *	/
2. Изработка на Методологија за процена на ризици (заедничка активност со МИОА за која ќе се бара експертска и финансиска помош од меѓународни организации и нема да се користат финансиски средства од Агенцијата)*	/
3. Проширување на Систем за сајбер-безбедносен надзор над мрежни инфраструктури	25.000.000,00 ден
4. Систем за надзор над јавен веб (.gov.mk и .mk)	6.000.000,00 ден
5. Систем за управување со компјутерски инциденти и сајбер безбедностни настани и информации **	6.000.000,00 ден
6. Фишинг кампањи и едукација	500.000,00 ден

** Активности од 2022 што продолжува во 2023 година, првично со буџет на АЕК за 2022 година

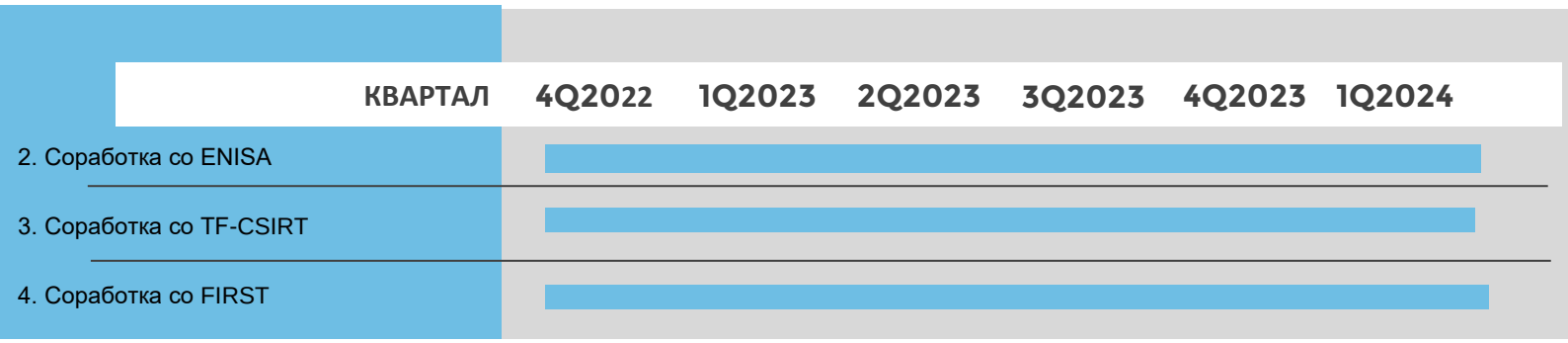
(Ц4) ПРЕСТАВУВА ОФИЦИЈАЛНА НАЦИОНАЛНА ТОЧКА ЗА КОНТАКТ И РАЗМЕНА НА ИНФОРМАЦИИ (ИЗВЕШТАИ ЗА ИНЦИДЕНТИ, РАНЛИВОСТ ИТН.) ЗА ВНАТРЕ ВО РАМКИТЕ НА ДРЖАВАТА КАКО И ЗА НАДВОР ОД НЕА СО НАЦИОНАЛНИТЕ/ВЛАДИНИ CIRT-ОВИ ОД ДРЖАВИТЕ ВО РЕГИОНОТ И ПОШИРОКО.
KGI 4.1 Членство во меѓународни организации KPI 4.1.1 Членство во FIRST, TF-CSIRT и др. KPI 4.1.2 Учество во форуми, вежби и конференции организирани од меѓународни организации **KGI 4.2 Регионална и меѓународна соработка** KPI 4.2.1 Договори за соработка со национални/владини и други CSIRT и безбедносни тимови во регионот **KGI 4.3 Информирање на јавноста за MKD-CIRT** KPI 4.3.1 Објави со совети за заштита испратени до весници, телевизии и портали KPI 4.3.2 Организација на јавни состаноци **KGI 4.4 Национална соработка и координација** KPI 4.4.1 Организација на работилници за соработка, пријава на инциденти и развој на секторски CSIRTови

KGI 4.1. Членство во меѓународни организации

Исполнувањето на оваа цел ќе се реализира со членство на MKD-CIRT како национален CSIRT на Република Северна Македонија во меѓународни организации:

- Барање за соработка со ENISA со предлог за вклучување на MKD-CIRT во размената на информации и соработката што ENISA ги обезбедува на другите национални CIRT-ови, како известувања, најдобри практики, работни групи, вежби и настани.
- Соработка со FIRST. Во 2020 година MKD-CIRT успеа да добие учество во програма за поддршка на FIRST (Fellowship program). FIRST како форум на CIRT тимови нуди помош во комуникацијата меѓу одделни CIRT-ови преку нивно запознавање или преку користење на воспоставената инфраструктура и системи за споделување на информации и соработка. Во 2022 година MKD-CIRT стана полноправен член во FIRST. Оваа соработка има основна цел да го забрза процесот на справување со компјутерските безбедносни инциденти.
- Континуирана соработката со TF-CSIRT Trusted Introducer. MKD-CIRT како Национален CSIRT на Република Северна Македонија е акредитиран член во ова меѓународно здружение. На овој начин MKD-CIRT веќе има воспоставено високо ниво на доверба во комуникацијата со останатите национални CSIRT тимови кои се исто така членови. Во 2023 година ќе продолжи соработката со ова здружение преку размена на информации со другите членови и активно учество на MKD-CIRT во настаните и обуките кои ги организира TF-CSIRT.

Период за реализација



Финансиски трошоци

1. Членство во меѓународни организации и котизации за учество на меѓународни настани	300.000,00 ден.

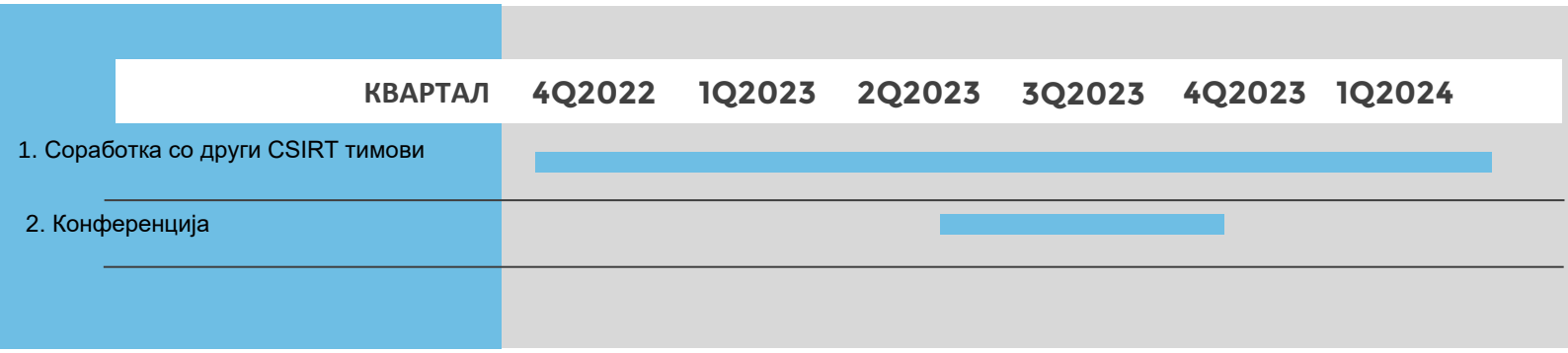
KGI 4.2. Регионална и меѓународна соработка

Продолжена и засилена активност за соработка со национални и владини CIRT и други безбедносни тимови и организации кои работат во областа на сајбер-безбедност од земјите во регионот и пошироко. Активноста е отпочната во 2016 и MKD-CIRT континуирано иницира соработка со тимови и организации од други земји со можност за нејзино официјализирање преку потпишување на договори за соработка во делот на:

- Размена на информации, известувања и алармирање за безбедносни ранливости и инциденти;
- Соработка, координација и заемна помош во справување со меѓународни безбедносни инциденти и закани;
- Учество на локални експерти од MKD-CIRT и конституентите во регионални работилници и вежби за сајбер безбедност;
- Организација на годишна меѓународна конференција со фокус и учество на национални и секторски CIRT-ови од други земји. Конференцијата има за цел да се разменат искуства со тимови од регионот, потпишување на меморандуми за билатерална и мултилатерална соработка во делот на споделување на информации и координација на активностите во справување со компјутерски безбедносни инциденти и закани. Конференцијата ќе има и едукативна компонента, со предавања од експерти од тимовите со цел едукација и јакнење на капацитетите на тимовите-учесници на конференцијата. Конференцијата е планирано да се реализира во соработка со други домашни и меѓународни организации.
- За реализација ќе се користат средства од Агенцијата и ќе се побара дополнително помош од меѓународни организации

Оваа активност е согласно точка 1.1.4 од АПССБ.

Период за реализација



Финансиски трошоци

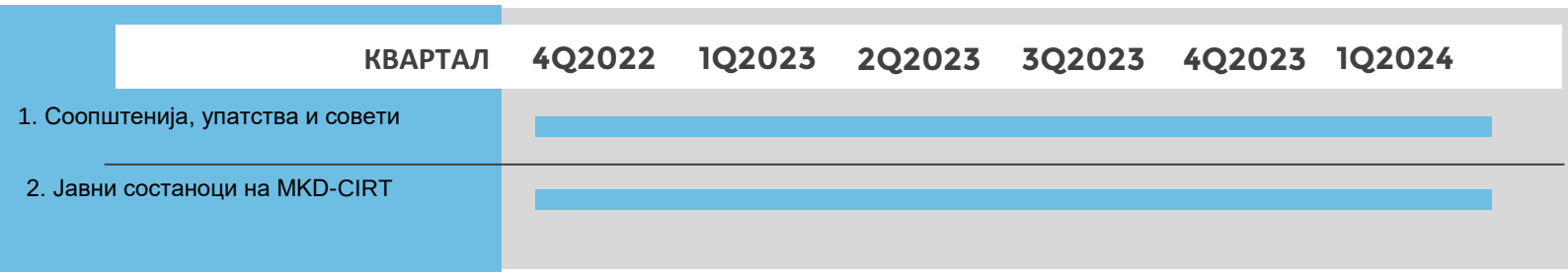
1. Конференција, национален натпрева ри национална вежба за кооридинација и одговор по инциденти - Хакатон CIRT	2.000.000,00 ден.

KGI 4.3. Информирање на јавноста за MKD-CIRT

Информирање на јавноста во Република Северна Македонија за MKD-CIRT како официјална национална точка за координација и размена на информации ќе се реализира со:

- испраќање на соопштенија до медиумите и континуирано информирање на јавноста за безбедносните закани и начини за заштита преку социјални мрежи, испраќање на текстови до новински агенции и со учество на членовите на тимот на MKD-CIRT на собири и настани во државата и странство.
- информирање на конституентите и организациите од јавниот и приватниот сектор за MKD-CIRT и неговите услуги преку презентации на услугите и активностите на MKD-CIRT на јавни состаноци, состаноци со здруженија и испраќање на соопштенија и информации за начинот на пружање на услугите и за начинот на воспоставување на соработка. Во 2023 година е планирано одржување на јавни состаноци, работилници, вебинари со покани за учество испратени до сите конституенти и лица задолжени за информацискатa безбедност во јавниот и владиниот сектор, како и за граѓаните и приватниот сектор.

Период за реализација



Финансиски трошоци

1. Организација на јавни состаноци – нема трошоци, за организација ќе се користи поддршка достапна во Агенцијата (ќе се користат просторни, технички и финансиски средства од Агенцијата). Дополнително ќе се побара помош од меѓународни организации	/

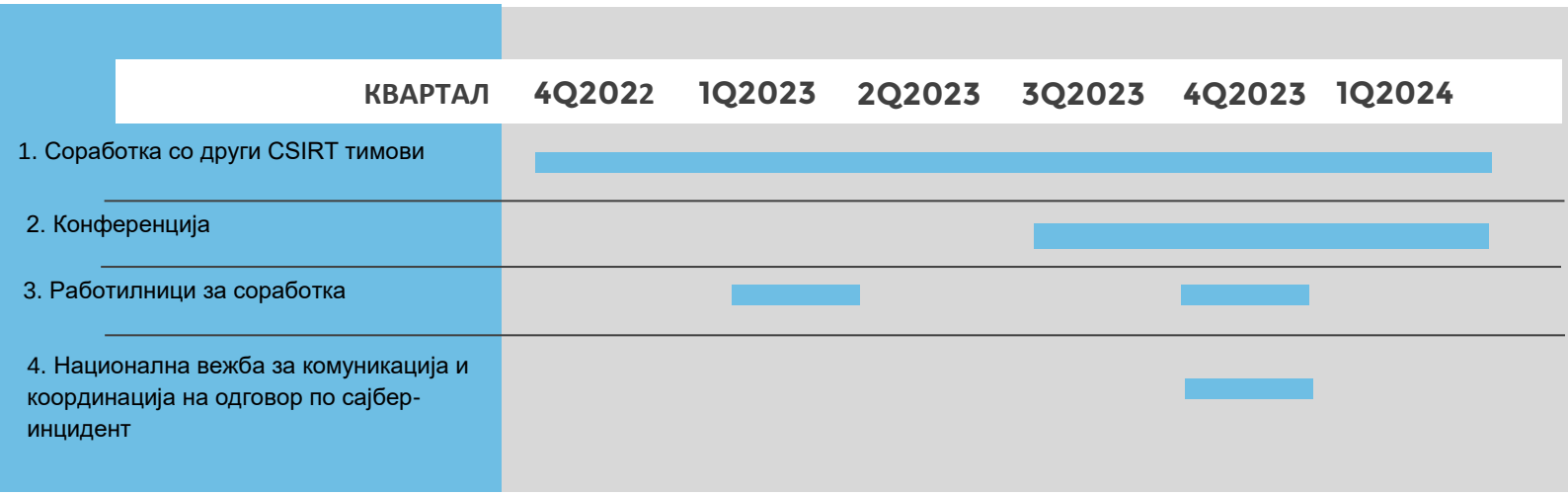
KGI 4.4. Национална соработка и координација

Националната соработка и координација има за цел јакнење на капацитетите во нашата земја за одговор на инциденти и соработка.

- Организација на годишна национална вежба за комуникација и координација по сајбер-инциденти – во врска со член 26-а од ЗЕК и задача 4.9.3 од АПССБ. Оваа активност се планира да се реализира заедно со планираната годишна конференција.
- Организација на работилници за соработка, пријава на инциденти и развој на секторски CSIRTови - во врска со задача 1.1.4 од АПССБ

Оваа активност е согласно член 26-а од Законот за електронските комуникации и точка 1.1.4 од АПССБ.

Период за реализација



Финансиски трошоци

1. Трошоци за службени патувања (превоз и сместување), ова е дел од вкупниот буџет на Агенцијата за 2023 година	/

2. Национална вежба за комуникација координација на одговор по сајбер-инциденти, како дел од конференција и Национален натпревар	2.000.000,00 ден.
3. Работилници за соработка	/

(Ц5) КОНСТИТУЕНТИТЕ НАВРЕМЕНО ДА ГИ ИНФОРМИРА, ИЗВЕСТУВА, ДА ИМ ОБЕЗБЕДУВА БЕЗБЕДНОСНИ СОВЕТИ, ИНФОРМАЦИИ ЗА РАНО ПРЕДУПРЕДУВАЊЕ И ДА ДЕЛУВА КАКО ЦЕНТРАЛНА ТОЧКА ЗА ПРАШАЊАТА ОД ОБЛАСТА НА САЈБЕР БЕЗБЕДНОСТА.
KGI 5.1 Навремено информирање KPI 5.1.1 Споделени информации KPI 5.1.2 Достапност на системот за размена на информации за штетен софтвер / Malware Information Sharing Platform MISP KGI 5.2 Совети и информации за рано предупредување KPI 5.2.1 Објавени информации преку MISP, веб-страницата, Twitter, Facebook и LinkedIn

KGI 5.1. Навремено информирање

Конституентите ќе се информираат навремено со обезбедување на комуникација преку безбедносни канали и тоа :

- континуирана достапност, подобрување и надградба на платформите за комуникација со констинуентите и граѓаните со MKD-CIRT (телефон, е-маил, факс, писмен допис, web итн).
    - веб страниците наменети за совети, рано предупредување како и за општи информации од областа на сајбер безбедноста
    - PGP-енкриптирана емаил комуникација
    - Систем за дистрибуција на информации до конституентите – Malware Information Sharing Platform
- освен традиционалните комуникациски канали, дистрибуцијата на помалку критични или помалку чуствителни (пред се јавни) информации кон своите конституенти и јавноста преку социјални мрежи (Facebook, Twitter)., со цел подигнување на јавната свест за сајбер безбедноста

Во 2017 година MKD-CIRT постави Систем за размена на информации за штетен софтвер, закани, ризици и инциденти – Malware Information Sharing Platform. Системот ќе продолжи да се користи и во 2023 година за насочена дистрибуција на информации и при координација на одговор на ризици и инциденти.

KGI 5.2. Рано предупредување

Во 2017 година MKD-CIRT постави систем за размена на информации со конституентите – Malware Information Sharing Platform MISP. Овој систем ќе продолжи да се користи и во 2023 година како ефикасен начин за рано предупредување на конституентите преку навремена и насочена дистрибуција на информации за нови ризици, штетен софтвер, инциденти и најдобри практики.

Секој конституент е приклучен на системот преку своите административни и технички контакти и системот овозможува споделување на структурирани прегледни информации кои можат да се искористат и од страна на ИКТ системите на конституентите – овозможена е Machine 2 Machine комуникација. На овој начин конституентите можат да ги применат информациите во своите Intrusion Prevention and Detection системи.

Во 2023 година се планира овој систем да се поврзе со други инстанци од други земји и меѓународни организации како FIRST и NATO, со што ќе се подобри навремената размена на информации.

Период за реализација

КВАРТАЛ	4Q2022	1Q2023	2Q2023	3Q2023	4Q2023	1Q2024
1. Навремено информирање						
2. Рано предупредување						

Финансиски трошоци

За реализација на овие активности нема дополнителни финансиски трошоци	/

(Ц6) ЦЕЛОСНО СОРАБОТУВА И РАЗМЕНУВА ИНФОРМАЦИИ СО ИНСТИТУЦИИТЕ ОД ДРЖАВАТА НАДЛЕЖНИ ЗА СПРОВЕДУВАЊЕ НА ЗАКОНИТЕ, А ОСОБЕНО СО ОНИЕ ОД ОБЛАСТА НА САЈБЕР КРИМИНАЛОТ
KGI 6.1 Соработка со институции во државата надлежни за спроведување на законите
KPI 6.1.1 Потпишани договори за соработка со надлежни министерства и други организации во државата
KPI 6.1.2 Реализирана обука за членовите на тимот на MKD-CIRT за правилно ракување со електронски докази и артефакти, во областа на дигитална форензика

KGI 6.1. Соработка со институции во државата

Во 2020 година Владата ги задолжи сите институции од државната управа, а им укажа на сите институции кои не се органи на државната управа да се зачленат во MKD-CIRT. Оваа активност ќе продолжи и во 2023 година. Националниот центар за одговор на компјутерски инциденти целосно ќе биде посветен за соработка и размена на информации со останатите државни институции кои се надлежни за спроведување на законската рамка на Република Северна Македонија за технички и организациски мерки за обезбедување на тајност и заштита на обработка на податоци, безбедност на мрежи, заштита на лични податоци како и од областа на сајбер криминалот. Реализација на овие активности ќе се врши преку:

- Континуирано зачленување на сите организации од јавниот и владиниот сектор, согласно точка 5.1.3 од АПССБ
- Иницирање на соработка со надлежни министерства и организации во државата
- Во 2023 година MKD-CIRT и понатаму ќе биде отворен за соработка со Министерството за информатичко општество и администрација како ресорно министерство во делот на изработката и спроведување на Акциски план и законски и подзаконски решенија, како и во делот на ревизија на постојните стратешки документи, акциски планови и законски и подзаконски решенија. MKD-CIRT и Агенцијата за електронски комуникации се спремни да дадат активен стручен придонес и да учествуваат во активностите за транспонирање на европската директива - The directive on security and information systems (NIS Directive) 2016/1148.

Период за реализација

КВАРТАЛ	4Q2022	1Q2023	2Q2023	3Q2023	4Q2023	1Q2024
1. Соработка со институциите во Република Северна Македонија						

Финансиски трошоци

За реализација на овие активности нема дополнителни финансиски трошоци	/

(Ц7) КОНТИНУИРАНО ДА РАЗМЕНУВА ИНФОРМАЦИИ, ЗНАЕЊЕ И ИСКУСТВА СО КОНСТИТУЕНТИТЕ, ДА УТВРДУВА БЕЗБЕДНОСНИ НАЈДОБРИ ПРАКТИКИ/УПАТСТВА
KGI 7.1 Размена на информации знаења и искуства со конституенти
KPI 7.1.1 Организирање на состаноци со конституенти
KPI 7.1.2 Организација на обуки за конституенти за пријава на инциденти
KPI 7.1.3 Организација на обуки за конституенти за управување со ризиците
KPI 7.1.4 Организација на обуки за конституенти за процена на ранливости
KPI 7.1.5 Организација на вежба за координација на одговор по инцидент со конституенти
KGI 7.2 Утврдување на безбедносни најдобри практики и упатства
KPI 7.2.1 Објава на упатства и најдобри практики наменети за конституенти
KGI 7.3 Center of Excellence for Cyber security
KPI 7.3.1 Лабораторија и едукативен центар за анализа на штетен софтвер и дигитална форензика, што ќе се користи и за изведување на обуки и сајбер-вежби.
KPI 7.3.2 Изработка и реализација на обуки за членовите на тимот и конституентите

KGI 7.1. Соработка со конституентите

Обезбедување на кадар кој ќе може технички да одговори на сите предизвици за одговор на компјутерски инциденти е важна компонента во работењето на MKD-CIRT. За таа цел неопходно е доекипирање на тимот на центарот и континуирана едукација на членовите на тимот.

Едукација на вработените ќе биде преку само едукација со користење на едукативни материјали достапни на интернет, преку посета на специјализирани курсеви за CIRT тимови организирани од меѓународни организации и провајдери (пр. TERENA/GEANT TRANSIT I, TRANSIT II и др.) но и со размена на искуства со локалните, регионалните и меѓународните центри за одговор на компутерски инциденти преку работилници, семинари и вежби.

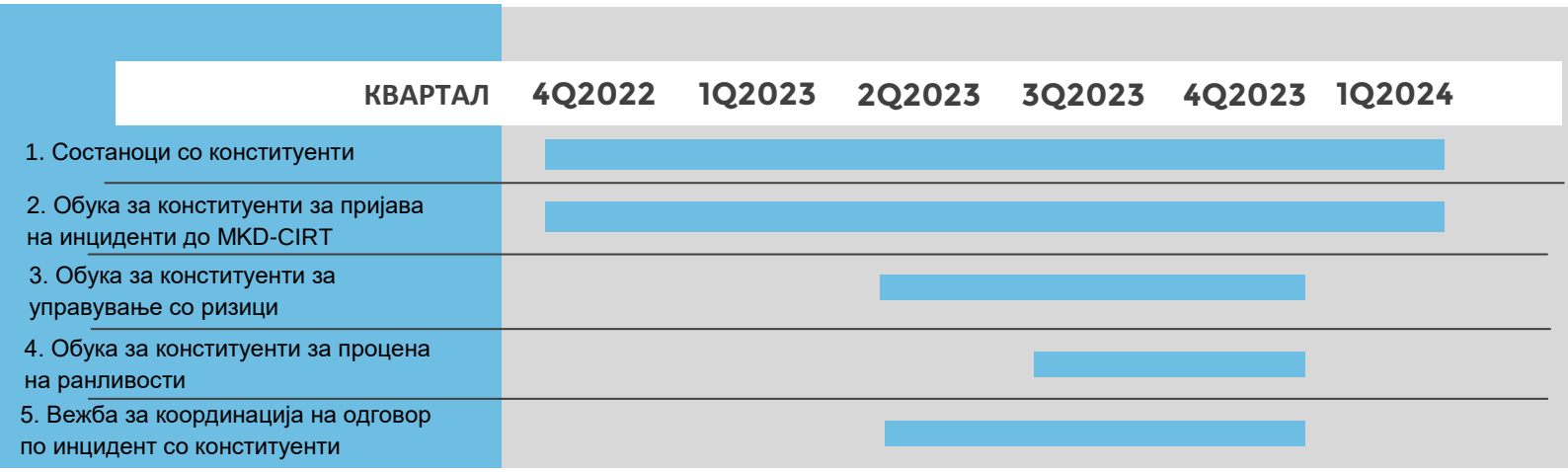
MKD-CIRT во 2023 година континуирано ќе разменува информации, знаење и искуство со конституентите, ќе утврдува безбедносни најдобри практики/водичи и истите ќе ги објавува. Во таа насока, MKD-CIRT континуирано ќе обезбедува едукација и обуки за вработените и за конституентите.

Едукацијата на вработените во MKD-CIRT е во насока на здобивање со знаења и вештини во делот на информацискатa безбедност, управување со информациска безбедност, управување со процес за справување со компјутерски безбедносни инциденти, penetration testing, откривање и анализа на ранливости и форензика по настанат инцидент. Потврда на стекнатите знаења ќе се врши преку сертификација на вработените согласно меѓународно признаените сертификации од страна на ENISA, ITU и EU, во делот на:

- Управување со информациска безбедност и Управување со процесите за справување со безбедносни инциденти, како на пример ISC2 CISSP (Certified Information Security Professional), ISACA CISM (Certified Information Security Manager), EC Council CCSO (Certified Chief Information Security Officer), EC Council CIH (Certified Incident Handler)
- Форензика, Penetration testing и енкрипција, како на пример EC Council CES/CEH/CHFI (Certified Encryption Specialist/Certified Ethical Hacker/Computer Hacking Forensics Investigator)
- Анализа и управување со ризици како на пример ISO 27001 Implementer, ISACA CRISC (Certified in Risk and Information System Control) и ISO 27005 (Risk Management)

Едукација на конституентите е во насока на јакнење на капацитетите на лицата и тимовите задолжени за информацискатa безбедност на страна на конституентите. За исполнување на оваа цел MKD-CIRT во 2023 година ќе организира работилници за конституентите.
Оваа активност е согласно точка 5.1.10 од АПССБ.
Детален опис на работилниците е даден во активностите за исполнување на следната цел – Ц8.

Период за реализација



Финансиски трошоци

1. Едукативни материјали и видеа и промоција за сајбер-безбедност - CIRT	1.200.000,00 ден.
2. Обука за конституенти за процена на ризици, ранливости и сајбер безбедност *	/

*Финансиски трошоци (активности што се финансираат од буџетот на Агенцијата и реализацијата зависи од достапноста на средства)

KGI 7.2. Безбедносни најдобри практики и упатства

Во 2023 година MKD-CIRT ќе објавува информации, упатства и најдобри практики наменети за конститунетите во делот на процена на ризик, процена на ранливости на системите и мрежите на конституентите и упатства за ублажување на ефектите од актуелни сајбер закани и за надминување на откриени ранливости.

Период за реализација

КВАРТАЛ	4Q2022	1Q2023	2Q2023	3Q2023	4Q2023	1Q2024
1. Безбедносни најдобри практики и упатства						

Финансиски трошоци

За реализација на овие активности нема дополнителни финансиски трошоци	/

KGI 7.3. Centre of Excellence for Cybersecurity

Активност пренесена од програмата за работа на MKD-CIRT за 2021/22 година. Во 2020 година MKD-CIRT имплементираше опрема за проверка на штетен софтвер и дигитална форензика која истовремено ќе се користи и како центар за едукација на вработените во националниот центар и кај конституентите. Во овој центар ќе се овозможи организирање на практични вежби, обуки и настава за конституентите на MKD-CIRT како и организација на јавни настани во просториите на Центарот. Дополнително ќе се овозможи користење на Центарот за едукација при MKD-CIRT како лабораторија во која вработените во MKD-CIRT ќе можат да анализираат штетни софтвери. Развој и спроведување на едукативни активности во соработка со ФИНКИ, УГД и други факултети/универзитети во државата со кои АЕК/MKD-CIRT потпишува договори за соработка.

Период за реализација

КВАРТАЛ	4Q2022	1Q2023	2Q2023	3Q2023	4Q2023	1Q2024
1. Активности за едукација, анализи и истражување (Centre of Excellence for Cybersecurity)						

Финансиски трошоци

За овие активности нема финансиски трошоци. Потребни средства би се обезбедиле евентуално од буџет на АЕК	/

(Ц8) ОБЕЗБЕДУВА ПОМОШ ВО ПРОЦЕСОТ НА ВОСПОСТАВУВАЊЕ НА ИНТЕРНИ ЦЕНТРИ ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ НА ГОЛЕМИТЕ ОРГАНИЗАЦИИ КОИ УПРАВУВААТ СО КЛУЧНИ/КРИТИЧНИ ИНФОРМАЦИСКИ ИНФРАСТРУКТУРИ (ЈАВНИ И ПРИВАТНИ) ВО РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
Исполнување на оваа цел ќе се врши со реализација на активностите дефинирани во: KPI 1.1.1, KPI 7.1.2, KPI 7.1.3 и KPI 7.1.4

Една од активностите на националниот центар за одговор на компјутерски инциденти е поддршка при воспоставување на интерни центри за одговор на компјутерски инциденти, особено на организации кои управуваат со клучни/критични информациски инфраструктури, и на барање од конституентите за учество и давање на помош во самиот процес на воспоставување на интерни центри за одговор на компјутерски инциденти, особено на организации кои управуваат со клучни/критични информациски инфраструктури.

Ова е од големо значење заради повеќе причини:

- Зголемување на бројот на обучен технички персонал одговорен за одговор на компјутерски инциденти
- Подобрување на одржувањето и превентивно делување на ниво на институција за обезбедување на заштита против компјутерски инциденти
- Обезбедување на брза и ефикасна реакција при кризни ситуации
- Подигање на нивото на свест за сајбер безбедност на поединечни институции

За исполнување на оваа цел во 2023 година MKD-CIRT ќе ги преземе следните активности:

- Организирање на работилници за конституентите на теми:
  - Соработка и воспоставување на секторски тимови
  - Управување со процесот за справување со инциденти

- Методи за самостојна процена на ранливости на информациските системи и мрежи и процена на ризиците во организациите на конституентите, базирани на ISO 27005 или други меѓународни стандарди
- Имплементација на најдобри пракси за воведување на технички и организациски мерки за безбедност на мрежи и системи во организацијата на конституентот
- Процена на ризиците во организацијата на конституентот, со одредување на критичност на ИКТ системите

Оваа активност е согласно точка 1.1.4 од АПССБ.

(Ц9) ПОДИГАЊЕ НА СВЕСТА КАЈ ГРАЃАНИТЕ ЗА НЕГАТИВНИТЕ ЕФЕКТИ НА САЈБЕР ЗАКАНИТЕ И КОМПЈУТЕРСКИОТ КРИМИНАЛ
KGI 9.1 Совети за безбедно работење на интернет
KPI 9.1.1 Изработка, објава и дистрибуција на брошури за Безбедно работење на интернет
KPI 9.1.2 Сајбер-шампион, онлајн обука и квиз
KPI 9.1.3 Објава на едукативни содржини во кампања ЗАСТАНИ. РАЗМИСЛИ. ПОВРЗИ СЕ
KPI 9.1.4 Одговорно работење на Интернет
KPI 9.1.5 Online обуки за раководен персонал во јавен и приватен сектор и јавна администрација

KGI 9.1. Безбедно користење на интернет

Подигнување на свеста на граѓаните за сајбер безбедноста е важна превентивна мерка за борба против компјутерските инциденти и компјутерскиот криминал. Оваа услуга која е дел од услуги за управување со квалитетот на безбедноста во 2023 година ќе се реализира преку следните активности:

- Испитување на јавно мислење со цел да се добие слика за информираноста на граѓаните за сајбер заканите и користењето на интернет услуги. Во 2023 се планира реализација на четврт циклус од испитувањето. Во 2020/21 година, планираното испитување не е реализирано заради неможноста да се спроведе анкетирање во живо.
- Изработка, објава и дистрибуција на брошури за Безбедно работење на интернет.

Оваа активност е согласно точка 2.3.1 од АПССБ.

- Објава на основни едукативни содржини за сајбер безбедност на официјалната страница на националниот центар https://mkd-cirt.mk, како и на социјалните мрежи Facebook, Twitter, LinkedIn

ЗАСТАНИ. РАЗМИСЛИ.ПОВРЗИ СЕ

Во 2017 година MKD-CIRT се приклучи на глобална кампања за подигање на свеста која се реализира под името „ЗАСТАНИ. РАЗМИСЛИ. ПОВРЗИ СЕ“. “STOP. THINK. CONNECT” е глобална кампања за едукација и информирање за безбедноста на интернет за да им помогне на сите дигиталните граѓани во безбедното работење на интернет. Пораката базирана на истражување беше создадена во 2009 година од коалиција на приватни компании, непрофитни организации и владата на САД под лидерство на Националната асоцијација за сајбер безбедноста (NCSA) и од Анти-фишинг работната група (APWG). Во 2023 година MKD-CIRT ќе продолжи со објава на едукативни материјали и совети за информациска безбедност кои се достапни преку меѓународна соработка.

Национален натпревар - Хакатон

До крајот на 2023 година MKD-CIRT ќе се обиде да реализира проект за спроведување на национален натпревар за откривање на слабости и ранливости во виртуелна околина на кој ќе можат да учествуваат поголем број млади во РСМ, индивидуално или организирани во тимови од 3+ луѓе. Цел е да се информираат граѓаните за значењето на заканите во on-line просторот како и да се вклучат пред се младите од факултетите и средните училишта кои се целна група на учесници на натпреварот. Реализацијата на проектот е дел од конференција и Национална вежба за комуникација и координација на одговор по сајбер-инциденти. Како основа се предлага да се воспостави нова (или користи услуга за постојна) онлајн платформа за едукација, обуки тестирање на која покрај поставување на новии сосдржини ќе се изврши и консолидација на едукативните и содржините за тестирања и квизови што веќе се изработени ио јавно достапни. Проектот опфаќа:

- користење на on-line платформа на која ќе се спроведува натпреварот,
- изработка на сценарија (на пример capture the flag, blue team vs. red team, defending critical infrastructure)
- спроведување на јавна кампања за промоција на натпревар со едукативни елементи
- организирање на финален натпревар и пренос на настанот на Интернет
- Обезбедување на награди за најдобрите учесници

За реализација на оваа активност ќе се користат средства од АЕК по две ставки: Конференција со национален натпревар и национална вежба, и за Онлајн платформа за едукација и обуки, за што ќе се побара донаторска помош или дополнително дообезбедување на средства од буџет на АЕК.

Одговорно работење на Интернет

Проект од 2021/2022 кој продолжува во 2023 година, кој има за цел промоција за користење на алатка за само-оценување наменета за организациите од јавниот и приватниот сектор. Организациите самостојно би ја оцениле својата спремност и посветеност на имплементација на мерки за заштита во сајбер просторот. По нивна успешна оцена, тие би имале право да истакнат на своите портали ознака дека работат одговорно на Интернет. Од големо значење е поддршката за овој проект од МИОА и стопанските комори.

Сајбер-шампион

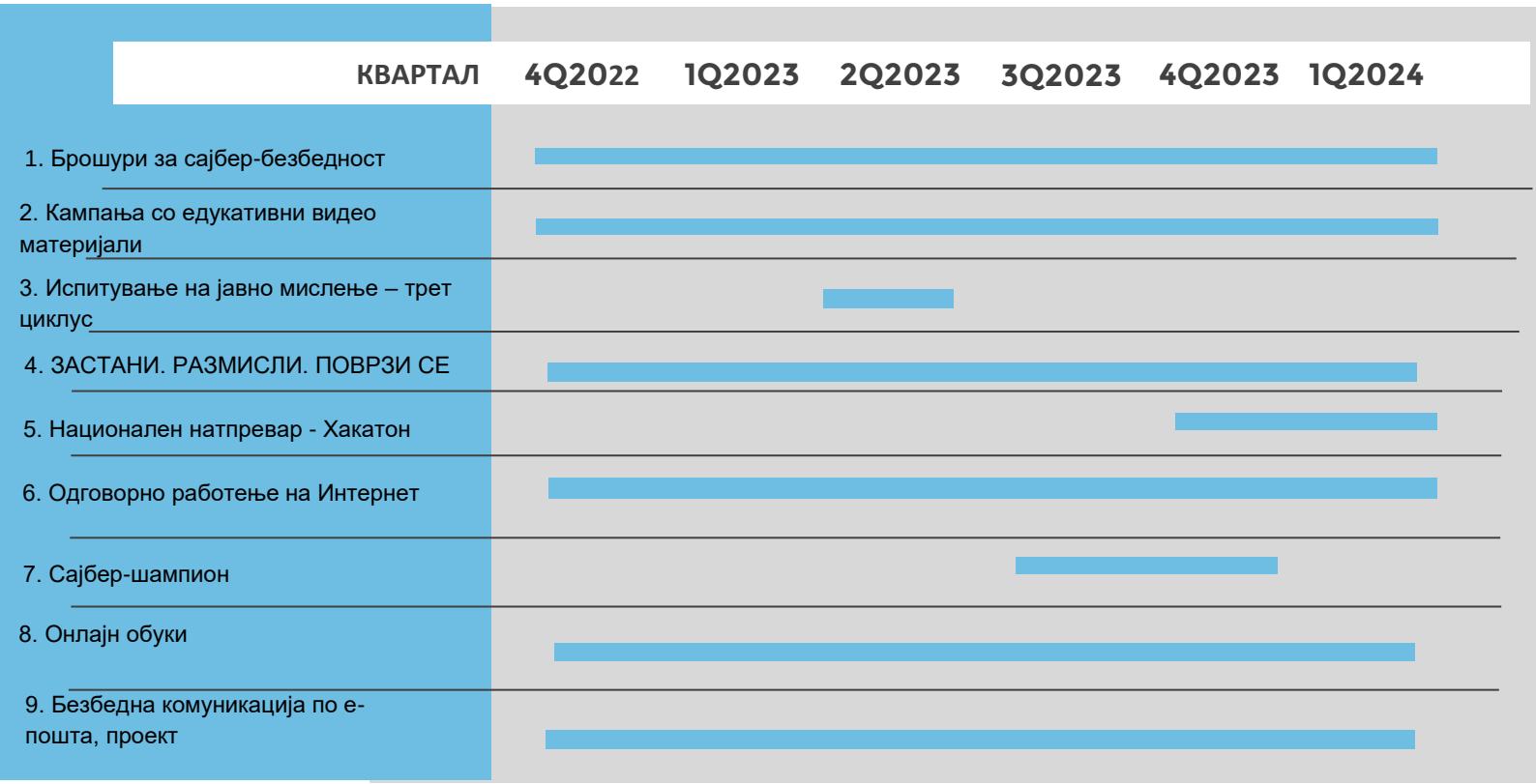
Проект наменет за online оценка на нивото на знаење и едукација на граѓаните, преку изработка на квиз и промоција.

Безбедна комуникација по е-пошта

Проект / услуга од 2020/21 година кој продолжува да се користи и надградува и во 2022/2023 година и има за цел воведување на безбедносни мерки во системите за електронска пошта во јавниот и владиниот сектор. Планирани надградби за анализа на заглавја на пораки по е-пошта, проверка на сертификати и протоколи за заштита, како и анализа на усогласеност со добра пракса и минимална група стандарди за комуникација.

Online обуки

Проект / услуга за изработка на курсеви и онлајн обуки наменети за граѓано, вработени во јавен и приватен сектор, администрацијата и менаџерскиот кадар од 2021/2022 година, со продолжување и изработка на нови едукативни онлајн содржини и обуки за одредени целни групи. За успешна реализација на овој проект од голема важност е поддршката од МИОА. Како дел од обуките, се предлага и фокус на сектор образование со посебен осврт на едукација на наставниот кадар и менаџментот на основните и средните училишта во државата – во координација со МОН и МИОА. Истото е основа за идни проектни активности за заштита и идентифукување на закани и инциденти и напади во секторот едукација, за што може да се предложат дополнителни проектни активности кои не се наведени во оваа верзија од документот. Овие активности се согласно точка 2.4.1 и 2.4.2 од АПССБ.



Финансиски трошоци

1. Брошури и упатства за безбедно користење на интернет – Услуги за копирање, печатење и издавање	500.000,00 ден.
2. Едукативни материјали, видеа и промоција за сајбер-безбедност - CIRT	1.200.000,00 ден.
3. Испитување на јавно мислење	300.000,00 ден.
4. ЗАСТАНИ. РАЗМИСЛИ. ПОВРЗИ СЕ (нема финансиски трошоци)	/
5. Национален натпревар – Хакатон*	/
7. Одговорно работење на интернет**	1.200.000,00 ден
8. Сајбер шампион – онлајн квиз *	615.000,00 ден.
9. Безбедна комуникација по е-пошта – пренесена реализација од 2022 година	925.000,00 ден.
10. Оналјн обуки	1.200.000,00 ден.

* За реализација на оваа активност ќе се побара донаторска помош или обезбедување на средства од Агенцијата.

7. Организација

7.1. Организација и расположливи ресурси

Националниот центар за одговор на компјутерски инциденти е формиран како посебна организациска единица во состав на Агенцијата за електронски комуникации.

Извадок од органограмот на внатрешна организација на АЕК е претставен на следната слика.

7.2. Човечки ресурси

Агенцијата за електронски комуникации за 2023 година има обезбедено финансиски средства за нови вработувања во насока на екипирање на MKD-CIRT. За националниот центар за одговор на компјутерски инциденти планирани се 5 работни места со структура претставена во следната табела

Работно место во систематизација	Стручна спрема	Шифра на работно место				
Раководител на Служба - Национален центар за одговор на компјутерски инциденти	ВСС	АЕК	01	01	Б02	1
Советник за одговор на компјутерски инциденти	ВСС	АЕК	01	01	В01	1
Советник за одговор на компјутерски инциденти	ВСС	АЕК	01	01	В01	1
Советник за одговор на компјутерски инциденти	ВСС	АЕК	01	01	В01	1
Советник за одговор на компјутерски инциденти	ВСС	АЕК	01	01	В01	1

Вработените во MKD-CIRT задолжително мора да поседуваат безбедносни сертификати за пристап до класифицирани информации издадени од Дирекцијата за безбедност на класифицирани информации согласно член 38 од Законот за класифицирани информации и согласно меѓународните препораки (ITU, ENISA, EU). Вработените во MKD-CIRT треба да поседуваат овластувања за обработка на лични податоци издадени од Агенцијата за електронски комуникации.

Кандидатите за работа во MKD-CIRT задолжително треба да поседуваат сертификат кој има поврзаност со информациска и комуникациска безбедност , додека предност ќе имаат кандидатите кои поседуваат меѓународно признаени сертификати од страна на ENISA, ITU и EU , како на пример ISC2 CISSP, ISACA CISM, ISACA CRISC, CCSO, CIH, CES, CEH, CHFI.

Согласно точка 7.1 од овој документ и по добиените резултати од функционалната анализа, во 2023 година MKD-CIRT ќе и препорача на Агенцијата за електронски комуникации да направи измена на систематизацијата во насока на обезбедување на дополнителни работни места во Националниот центар за одговор на компјутерски инциденти.

8. Финансиски план

Планираните финансиски средства за работа на Центарот за одговор на компјутерски инциденти се утврдени во предлогот на Годишниот Финансиски план на Агенцијата за електронски комуникации за 2023 година кој е составен дел на предлогот за Годишна програма за работа на Агенцијата за електронски комуникации за 2023 година. Во време на подготовка на овој документ, предлог-финансискиот план на Агенцијата за 2023 година се очекува да биде објавен за јавна расправа и документот да е достапен на www.aek.mk. Подолу во текстот се извадоци од предлогот за Годишен финансиски план на Агенцијата за електронски комуникации кој се однесува за работата на Националниот центар за одговор на компјутерски инциденти.

Извадок од предлог-годишен финансиски план на Агенција за електронски комуникации за 2023 година

1	**Адаптивна надградба на серверска и мрежна опрема за ЦИРТ со превентивно одржување**	**11.700.000,00 ден**	
2	**Услуги за копирање, печатење и издавање**	**500.000,00 ден.**	
3	**Конференција, Национална вежба и Национален натрпевар - Хакатон**	**2.000.000,00 ден.**	
4	**Членарини во меѓународни организации**	**2.000.000,00 ден.**	
5	**Маркетинг истражување на јавното мислење**	**300.000,00 ден**	
6	**Онлајн обуки**	**1.200.000,00 ден.**	
7	**Проект Сајбер-одговорна организација**	**1.200.000,00 ден.**	
8	**Проект Квиз Сајбер-шампион**	**600.000,00 ден.**	
9	**Систем за управување со компјутерски инциденти и сајбер безбедностни настани и информации**		
10	**Проширување на Систем за сајбер-безбедносен надзор над мрежни инфраструктури 2 дел**	**25.000.000,00 ден.**	
11	**Безбедна комуникација по е-пошта**	**925.000,00 ден.**	
12	**Систем за надзор на јавен веб и лиценци за алатки за MKD-CIRT**	**6.000.000,00 ден.**	-
13	**Фишинг кампањи и едукација**	**500.000,00 ден.**	
14	**Бруто плати**	**5.000.000,00 ден.**	

Појаснување:

1. Постапка почната во септември/октомври 2022, се пренесува во 2023
2. Планирани средства во 2022, се пренесуваат во 2023
3. /
4. /
5. Реализација по договор со вкупна вредност од 575.000,00 денари без ДДВ, за два циклуса на годишно испитување. Првото испитување е реалзиирано во 2022 година. Се очекува во 2023 година реалзиација на второто годишно испитување
6. /
7. Проект со почната реализација во 2022 година, се пренесува во 2023 година
8. /
9. Проект со почната реализација во 2022 година, се пренесува во 2023 година. Ова е тековна активност по договор од 2022 година, трошоци се за превентивно месечно одржување и надзор, но и по барање за адаптивни надградби и користење на часови за надворешна експертска помош при решавање на инциденти
10. Планирани трошоци во ребаланс на буџет на АЕК за 2022 година, се пренесуваат во 2023 година
11. Активност од 2022 која продолжува во 2023 година
12. Продолжување лиценца за две години, со дополнителни лиценци за алатки за скенирање и проверка на ранливости кај ИКТ системи

9. Заклучок

Во текот на 2023 година Агенцијата за електорнски комуникации ќе работи интензивно на исполнување на мисијата и поставените цели преку реализирање на предвидените активности.

Еден од главните предизвици и во оваа година ќе биде зголемувањето на бројот на вработени и екипирањето на Националниот центар за одговор на компјутерски инциденти и давање на поддршка на сите конституенти како и нивна едукација за ефикасно извршување на задачите.

Предуслов за квалитетно и навремено пружање на услугите на MKD-CIRT за конституентите и граѓаните на Република Северна Македонија е екипирање на тимот на MKD-CIRT. Нивната едукација и експертиза ќе бидат во насока на градење на доверба во квалитетот на MKD-CIRT кај конституентите и користење на услугите на MKD-CIRT како национален CSIRT на Република Северна Македонија.

Обезбедувањето на основните информации за подигнувањето на свеста на граѓаните за компјутерската безбедност и сајбер-криминалот, како и специјализираните online обуки планирани за 2023 година ќе биде основа за надградба и континуирано збогатување со нови содржини, подигање на јавната свест и отпорноста на општеството.

Во оваа година ќе продолжи засилена отворена комуникацијата со останатите центри за одговор на компјутерски инциденти и безбедносни тимови во регионот и пошироко.

10. Влегување во сила

Годишната програма за работа на Националниот центар за одговор на компјутерски инциденти влегува во сила по усвојувањето од страна на Владата на Република Северна Македонија.

Директор на

Агенција за електронски комуникации

Jeton Akiku

_____

Наш број 1802-3226/1
Скопје, 11.11.2022