Republika e Kosovës
Republika Kosova - Republic of Kosovo
Qeveria – Vlada – Government

UREDBU (KP) BR. 05/2024 O UNUTRAŠNJOJ ORGANIZACIJI I SISTEMATIZACIJI RADNIH MESTA U AGENCIJI ZA SAJBER BEZBEDNOST[1]

[1] Uredbe KP – Br. 05/2024 o Unutrašnjoj Organizaciji i Sistematizaciji Radnih Mesta u Agenciji za Sajber Bezbednosit, odobrio je Premijer, Odlukom Br.028/2024, dana 06.03.2024.

Premijer Republike Kosovo,

U skladu sa članom 94 (stav 10) Ustava Republike Kosovo, člana 17 (stav 2) Zakona br. 08/L-173 o Sajber Bezbednosti, član 28 (stav 3) Zakona br. 06/L113 o Organizaciji i Funkcionisanju Državne Uprave i Nezavisnih Agencija, u skladu sa članom 9 (stav 1 podstav 1.11) Zakona br. 08/L-117 za Vladu Republike Kosovo kao i član 9 (stav 7) Uredbe br. 01/2020 o Standardima Unutrašnje Organizacije i Sistematizaciji Radnih Mesta i Saradnji u Institucijama Državne Uprave i Nezavisnim Agencijama,

Donosi:

UREDBU (KP) BR. 05/2024 O UNUTRAŠNJOJ ORGANIZACIJI I SISTEMATIZACIJI RADNIH MESTA U AGENCIJI ZA SAJBER BEZBEDNOSTI

POGLAVLJE I
OPŠTE ODREDBE

Član 1
Cilj

Ova Uredba ima za cilj utvrđivanje unutrašnje organizacije i sistematizaciju radnih mesta u Agenciji za sajber bezbednost.

Član 2
Delokrug

1. Ovu uredbu sprovodi Agencija za sajber bezbednost.

2. Dužnosti i odgovornosti Agencije su utvrđene relevantnim Zakonom o sajber bezbednosti.

POGLAVLJE II
UNUTRAŠNJA ORGANIZACIJA I SISTEMATIZACIJA RADNIH MESTA U AGENCIJI ZA SAJBER BEZBEDNOST

Član 3
Misija Agencije za sajber bezbednost

Misija Agencije za sajber bezbednost je da zaštiti kritičnu nacionalnu infrastrukturu, unapredi sajber bezbednost građana i preduzeća proaktivnim sprečavanjem sajber napada i stvaranjem bezbednog sajber prostora u Republici Kosovo.

Član 4
Organizaciona struktura Agencije

1. Organizaciona struktura Agencije je sledeća:

1.1. Kancelarija Izvršnog direktora;

1.2. Departmani;

1.3. Divizije.

2. Broj zaposlenih u Agenciji je trideset osam (38).

Član 5
Kancelarija Izvršnog direktora

1. Kancelariju Izvršnog direktora čine:

1.1. Izvršni direktor;

1.2. Stručno osoblje;

1.3. Pomoćno osoblje.

2. Dužnosti i odgovornosti Izvršnog direktora utvrđuju se relevantnim Zakonom o sajber bezbednosti, Zakonom o organizaciji i funkcionisanju državne uprave i nezavisnih agencija, relevantnim Zakonom o javnim službenicima i drugim važećim zakonodavstvom.

3. Dužnosti i odgovornosti stručnog i pomoćnog osoblja Kancelarije Izvršnog direktora utvrđuju se relevantnim zakonodavstvom o javnim službenicima.

4. Broj zaposlenih u Kancelariji Izvršnog direktora je šest (6).

Član 6
Departmani i divizije Agencije

1. Departmani i divizije Agencije su:

1.1. Nacionalni centar za prevenciju i reagovanje na sajber incidente:

1.1.1. Divizija za analizu i prevenciju incidenata;

1.1.2. Divizija za upravljanje incidentima;

1.2. Departman za standarde i nadzor:

1.2.1. Divizija za standarde i politiku;

1.2.2. Divizija za nadzor i praćenje;

1.3. Departman za usluge sajber bezbednosti:

1.3.1. Divizija za sertifikaciju opreme i usluga;

1.3.2. Divizija za tehničke i savetodavne usluge;

1.3.3. Divizija za unutrašnje IKT sisteme.

Član 7
Nacionalni centar za prevenciju i reagovanje na sajber incidente

1. Nacionalni centar za prevenciju i reagovanje na sajber incidente ima za misiju identifikaciju i tretman sajber pretnji i rizika u cilju sprečavanja sajber napada, reagovanja i upravljanja sajber incidentima i sprečavanja njihovog širenja u većim razmerama.

2. Dužnosti i odgovornosti Nacionalnog centra za prevenciju i reagovanje na sajber incidente su:

2.1. obezbeđuje koordinaciju aktivnosti na nacionalnom nivou za otkrivanje, zaštitu i reagovanje na sajber napade, kao i sprovođenje nadzora, praćenja, identifikacije, analize, istrage i reagovanja na incidente sajber bezbednosti;

2.2. obavlja operativne funkcije sajber bezbednosti kao Tim Republike Kosovo za reagovanje na kompjuterske hitne slučajeve na nacionalnom nivou – nacionalni CERT;

2.3. odgovoran za rukovanje, upravljanje incidentima i ranjivostima, prevenciju incidenata, analizu pretnji, upravljanje rizikom i proces oporavka usluge nakon incidenta;

2.4. koordinira rad na rešavanju incidenata sajber bezbednosti sa nadležnim institucijama u oblasti sajber bezbednosti na nacionalnom i međunarodnom nivou;

2.5. predlaže ažuriranje liste sa vrstama sajber incidenata ili taksonomijom u skladu sa važećim zakonodavstvom;

2.6. kreira i vodi registar sajber incidenata i pretnji;

2.7. sprovodi istraživanja, analizira i ocenjuje sajber pretnje;

2.8. identifikuje, procenjuje i upravlja sajber rizicima;

2.9. predlaže *ad-hoc* timove koje odobrava Izvršni direktor, za brzo reagovanje na sajber incidente, za pomoć u situacijama kada operateri osnovnih usluga i pružaoci digitalnih usluga nemaju tehničke/ljudske kapacitete i kada se ispunjavaju kriterijumi koji su utvrđeni važećim zakonodavstvom;

2.10. daje preporuke za tehnička poboljšanja operaterima osnovnih usluga i pružaocima digitalnih usluga, u slučajevima kada se uoče slabosti;

2.11. kroz tim za brzo reagovanje Flash pruža konkretnu tehničku podršku u brzom rešavanju identifikovanih sajber pretnji i ranjivosti;

2.12. priprema godišnji izveštaj sa analizama, ocenama i prognozama o stanju sajber bezbednosti na nacionalnom nivou (sa akcentom na subjekte koji su u nadležnosti Agencije) i sa preporukama za povećanje nacionalne sajber stabilnosti.

3. Nacionalni centar za prevenciju i reagovanje na sajber incidente je ekvivalentna struktura Departmanu.

4. Direktor Nacionalnog centra za prevenciju i reagovanje na sajber incidente izveštava Izvršnom direktoru Agencije;

5. Nacionalni centar za prevenciju i reagovanje na sajber incidente sastoji se od dve divizije:

5.1. Divizija za analizu i prevenciju incidenata;

5.2. Divizija za upravljanje incidentima.

6. Broj zaposlenih u Nacionalnom centru za prevenciju i reagovanje na sajber incidente je dvanaest (12).

Član 8
Divizija za analizu i prevenciju incidenata

1. Divizija za analizu i prevenciju incidenata ima za misiju analiziranje i rešavanje sajber pretnji i rizika u cilju sprečavanje sajber napada.

2. Dužnosti i odgovornosti Divizije za analizu i prevenciju incidenata su:

2.1. identifikuje anomalije i slabosti u mrežnim i informacionim sistemima operatera osnovnih usluga i pružalaca digitalnih usluga, u skladu sa zakonodavstvom o sajber bezbednosti;

2.2. sprovodi kontinuirano istraživanje razvoja u oblasti sajber bezbednosti i preporučuje bezbednosna ažuriranja u slučaju otkrivanja slabosti i rizika koji mogu uticati na bezbednosnu ranjivost mrežnih i informacionih sistema;

2.3. šalje obaveštenja o poboljšanjima operaterima osnovnih usluga i pružaocima digitalnih usluga;

2.4. vrši testiranje ranjivosti, (v*ulnerability testing, pen-testing, itd.),* analizu rizika i procenu bezbednosti za operatere osnovnih usluga i pružaoce digitalnih usluga;

2.5. analizira i preporučuje implementaciju bezbednosnih specifikacija za informacione sisteme i mreže;

2.6. priprema i primenjuje sistem ranog upozoravanja za obaveštenja u slučaju neposrednih sajber incidenata, koji mogu imati uticaj ne samo na operatere osnovnih usluga i pružaoce digitalnih usluga, već i na preostali deo društva;

2.7. preko flash tima za brzo reagovanje:

2.7.1. Pruža konkretnu tehničku pomoć, a na zahtev operatera osnovnih usluga i pružaoca digitalnih usluga i direktnu podršku, u preduzimanju akcija za rešavanje pretnji i ranjivosti;

2.7.2. redovno i kontinuirano nadgleda dostupnost patch-ova za rešavanje pretnji i ranjivosti tako što održava stalni kontakt sa departmanima za bezbednost mrežnih i informacionih sistema i proizvođača opreme;

2.7.3. Proizvodi uputstva za primenu patch-ova i rešenja za rešavanje sajber pretnji i ranjivosti.

2.8. kreira i upravlja elektronskom platformom za razmenu informacija u realnom vremenu sa osnovnim operaterima usluga i pružaocima digitalnih usluga;

2.9. kreira i vodi registar sajber rizika i pretnji;

3. Rukovodilac Divizije za analizu i prevenciju incidenata izveštava direktoru Nacionalnog centra za prevenciju i reagovanje na sajber incidente.

4. Broj zaposlenih u Diviziji za analizu i prevenciju incidenata je pet (5).

Član 9
Divizija za upravljanje incidentima

1. Divizija za upravljanje sajber incidentima ima za misiju reagovanje i upravljanje sajber incidentima i sprečavanje njihovog širenja u većim razmerama.

2. Dužnosti i odgovornosti Divizije za upravljanje incidentima su:

2.1. prima obaveštenja o sajber incidentima od operatera osnovnih usluga i pružalaca digitalnih usluga, analizira prirodu incidenta i preduzima akcije za rukovanje i upravljanje incidentom u skladu sa važećim zakonodavstvom;

2.2. pruža tehničku pomoć u slučaju sajber incidenata, podržava njihovo rešavanje i analizu nakon incidenata;

2.3. pruža podršku za proces oporavka usluga nakon incidenta;

2.4. priprema detaljan izveštaj o incidentu i prosleđuje ga višoj hijerarhiji;

2.5. kreira i vodi registar sajber incidenata.

3. Rukovodilac Divizije za upravljanje incidentima izveštava direktoru Nacionalnog centra za prevenciju i reagovanje na sajber incidente.

4. Broj zaposlenih u Diviziji za upravljanje incidentima je šest (6).

Član 10
Departman za standarde i nadzor

1. Departman za standarde i nadzor ima za misiju nadzor nad sprovođenjem mera bezbednosti i pripremu procedura i tehničkih standarda koji su utvrđeni za operatere osnovnih usluga i pružaoce digitalnih usluga.

2. Dužnosti i odgovornosti Departmana za standarde i nadzor su:

2.1. prima i analizira izveštaje o proceni rizika od osnovnih operatera usluga i pružalaca digitalnih usluga;
2.2. ocenjuje sprovođenje organizacionih, fizičkih i bezbednosnih mera informaciono-komunikacionih tehnologija za mrežne i informacione sisteme kod operatera osnovnih usluga i pružalaca digitalnih usluga utvrđenih u skladu sa važećim zakonodavstvom;

2.3. traži od operatera osnovnih usluga i pružalaca digitalnih usluga da obezbede:

2.3.1. informacije neophodne za procenu bezbednosti njihove mreže i informacionih sistema, uključujući dokumentovane bezbednosne politike;

2.3.2. dokaze o efektivnoj primeni bezbednosnih politika, kao što su rezultati bezbednosne revizije koju su sprovele nadležne institucije, uključujući osnovne dokaze, koji moraju biti dostupni agenciji.

2.4. priprema godišnji plan inspekcijskog nadzora koji odobrava Izvršni direktor Agencije i sprovodi inspekcijski nadzor radi utvrđivanja sprovođenja mera bezbednosti u mrežnim i informacionim sistemima prema operaterima osnovnih usluga i pružaocima digitalnih usluga koji su utvrđeni važećim zakonodavstvom;
2.5. nakon procene informacija ili na osnovu rezultata bezbednosnih inspekcijskih nadzora, priprema obavezujuća uputstva za operatere osnovnih usluga za otklanjanje uočenih nedostataka, koje dostavljaju operaterima osnovnih usluga i pružaocima digitalnih usluga uz odobrenje Izvršnog direktora Agencije;

2.6. licencira revizore sajber bezbednosti i objavljuje licencirane subjekte na zvaničnoj internet stranici Agencije;

2.7. predlaže izmene tehničkih standarda i politika za sprovođenje od strane operatera osnovnih usluga i pružalaca digitalnih usluga u skladu sa važećim zakonodavstvom;

2.8. predlaže Izvršnom direktoru Agencije prekršajne sankcije za nesprovođenje obaveza utvrđenih važećim zakonodavstvom od strane operatera osnovnih usluga i pružalaca digitalnih usluga.

3. Direktor Departmana za standarde i nadzor izveštava Izvršnom direktoru Agencije;

4. Departman za standarde i nadzor se sastoji od dve divizije:

4.1. Divizija za standarde i politiku;

4.2. Divizija za nadzor i praćenje;

5. Broj zaposlenih u Departmanu za standarde i nadzor je osam (8).

Član 11
Divizija za standarde i politiku

1. Divizija za standarde i politiku ima za misiju identifikaciju i usklađivanje sa međunarodnim standardima i preispitivanje tehničkih postupaka i standarda koji su utvrđeni za operatere osnovnih usluga i pružaoce digitalnih usluga.

2. Dužnosti i odgovornosti Divizije za standarde i politiku su:

2.1. preispita standarde informacione bezbednosti, okvire usklađenosti i minimalne bezbednosne mere koje su obavezne za subjekte nadzora agencije, u skladu sa važećim zakonodavstvom i predlaže izmene podzakonskih akata kojima su oni utvrđeni;

2.2. identifikuje međunarodne i lokalne standarde bezbednosti informacija kao zajedničku osnovu za implementaciju nacionalnih zahteva, industrije i preduzeća, i po potrebi predlaže izmene podzakonskih akata;

2.3. doprinosi razvoju, prilagođavanju i primeni standarda i politika bezbednosti informacija od strane drugih javnih institucija;

2.4. kreira vodiče za primenu minimalnih mera bezbednosti i najbolje prakse u oblasti sajber bezbednosti;

2.5. pruža savete i uputstva o standardima i politikama za subjekte koji su pod nadzorom agencije;

2.6. licencira revizore sajber bezbednosti i objavljuje licencirane subjekte na zvaničnoj internet stranici Agencije;

3. Rukovodilac Divizije za standarde i politiku izveštava direktoru Departmana za standarde i nadzor;

4. Broj zaposlenih u Diviziji za standarde i politiku je tri (3).

Član 12
Divizija za nadzor i praćenje

1. Divizija za nadzor i praćenje ima za misiju nadzor i praćenje sprovođenja bezbednosnih mera koje su utvrđene važećim zakonodavstvom za operatere osnovnih usluga i pružaoce digitalnih usluga.

2. Dužnosti i odgovornosti Divizije za nadzor i praćenje su:

2.1. identifikuje, ažurira i vodi listu subjekata koji su pod nadzorom agencije;

2.2. ažurira i vodi listu glavnih službenika bezbednosti operatera osnovnih usluga i pružalaca digitalnih usluga;

2.3. prima i analizira izveštaje o proceni od operatera osnovnih usluga i pružalaca digitalnih usluga;

2.4. priprema obavezna uputstva i preporuke i prosleđuje ih na usvajanje;

2.5. proverava sprovođenje bezbednosnih zahteva u skladu sa važećim zakonodavstvom o sajber bezbednosti;

2.6. vrši sprovođenje mandata Agencije uključujući: komunikaciju, prekršajne sankcije i pripremu preporuke za ograničenje ili obustavu korišćenja ili pristupa mrežama i informacionim sistemima;

2.7. vodi podatke i dokumentaciju prikupljenu tokom procesa nadzora u skladu sa važećim zakonodavstvom;

2.8. priprema izveštaje sa detaljnom analizom o opštim trendovima i usklađenosti subjekata u nadležnosti Agencije, neusklađenosti, merama implementacije, pritužbama i izazovima.

3. Rukovodilac Divizije za nadzor i praćenje izveštava direktoru Departmana za standarde i nadzor.

4. Broj zaposlenih u Diviziji za nadzor i praćenje je četiri (4).

Član 13
Departman za usluge sajber bezbednosti

1. Departman za usluge sajber bezbednosti ima za misiju pružanje usluga sajber bezbednosti za građane, preduzeća i javne institucije, kao i upravljanje, administraciju i održavanje unutrašnjih IKT sistema i laboratorija u okviru Agencije.

2. Dužnosti i odgovornosti Departmana za usluge sajber bezbednosti su:

2.1. vrši sertifikaciju bezbednosti opreme i usluga informaciono-komunikacionih tehnologija, u slučajevima kada to zahtevaju javne institucije, u skladu sa važećim zakonodavstvom;

2.2. priprema ažuriranu listu pružalaca informacione tehnologije i komunikacione opreme i usluga koji su nepouzdani, u skladu sa važećim zakonodavstvom;

2.3. kreira i upravlja komunikacionom platformom sa građanima i preduzećima koja će biti u neprekidnoj službi (24/7) za prijavljivanje sajber incidenata;

2.4. odgovara zainteresovanim stranama kada traže objašnjenja ili savete o raznim sajber pretnjama;

2.5. priprema i objavljuje materijale za podizanje svesti za sve kategorije društva za zaštitu od sajber napada;

2.6. objavljuje informacije o sajber pretnjama i preventivnim merama;

2.7. izrađuje i vrši tehničko upravljanje internet stranicom Agencije.

3. Direktor Departmana za usluge sajber bezbednosti izveštava Izvršnom direktoru Agencije;

4. Departman za usluge sajber bezbednosti sastoji se od tri divizije:

4.1. Divizija za sertifikaciju opreme i usluga;

4.2. Divizija za tehničke i savetodavne usluge;

4.3. Divizija za unutrašnje IKT sisteme.

5. Broj zaposlenih u Departmanu za usluge sajber bezbednosti je dvanaest (12).

Član 14
Divizija za sertifikaciju opreme i usluga

1. Divizija za sertifikaciju opreme i usluga ima za misiju sertifikaciju opreme i usluga za javne institucije u cilju funkcionisanja u bezbednoj infrastrukturi za informacione i komunikacione sisteme.

2. Dužnosti i odgovornosti Divizije za sertifikaciju opreme i usluga su:

2.1. utvrđuje postupak sertifikacije, standarde i zahteve za analizu rizika lanca nabavke interne IKT opreme i usluga koje koriste javne institucije, u skladu sa administrativnim uputstvom o pravilima i procedurama za proces sertifikacije i pripremu liste opreme i usluga informaciono-komunikacionih tehnologija koje su nepouzdane;

2.2. vrši analizu i procenu opreme i usluga koje mogu predstavljati rizik za lanac nabavke;

2.3. vodi listu sertifikovanih poverljivih i nepouzdanih prodavaca i dobavljača opreme i usluga;

2.4. pregleda i primenjuje najbolje prakse u sertifikaciji proizvoda i usluga.

3. Rukovodilac Divizije za sertifikaciju opreme i usluga izveštava direktoru Departmana za usluge sajber bezbednosti.

4. Broj zaposlenih u Diviziji za sertifikaciju opreme i usluga je tri (3).

Član 15
Divizija za tehničke i savetodavne usluge

1. Divizija za tehničke i savetodavne usluge ima za misiju pružanje podrške i saveta građanima, preduzećima i institucijama da ne budu meta sajber napada.

2. Dužnosti i odgovornosti Divizije za tehničke i savetodavne usluge su:

2.1. upravlja komunikacionom platformu sa građanima, preduzećima i institucijama koje će biti u neprekidnoj službi (24/7) za prijavljivanje sajber incidenata;

2.2. priprema kampanje za podizanje svesti i objavljuje različite edukativne i nastavne materijale za zaštitu od sajber napada;

2.3. pruža tehničku podršku građanima i preduzećima kroz objavljivanje različitih materijala i alata;

2.4. razvija i pruža usluge javne sajber bezbednosti kao što su PDNS (Protective DNS) i analize zlonamernih softvera (malware).

3. Rukovodilac Divizije za tehničke i savetodavne usluge izveštava direktoru Departmana za usluge sajber bezbednosti.

4. Broj zaposlenih u Diviziji za tehničke i savetodavne usluge je pet (5).

Član 16
Divizija za unutrašnje IKT sisteme

1. Divizija za unutrašnje IKT sisteme ima za misiju podršku agenciji za obavljanje njenih funkcija kroz upravljanje unutrašnjim IKT sistemima i infrastrukturom.

2. Dužnosti i odgovornosti Divizije za unutrašnje IKT sisteme su:

2.1. upravlja i održava sve informaciono-komunikacione sisteme i laboratorije Agencije;

2.2. obezbeđuje optimalan rad i siguran pristup i u skladu sa politikom usvojenom na institucionalnom nivou u računarskim sistemima Agencije;

2.3. pruža tehničku podršku odgovarajući na zahteve korisnika računarske opreme u vezi sa nefunkcionisanjem jedne ili više komponenti opreme ili instaliranog softvera;

2.4. identifikuje potrebe i izrađuje tehničke specifikacije za nabavku opreme i softvera za potrebe Agencije;

2.5. organizuje testiranje i ocenjivanje bezbednosnih tehnologija i specifičnih aplikacija neophodnih za optimalno funkcionisanje Agencije;

2.6. pruža podršku za analizu, razvoj, implementaciju i održavanje baza podataka i aplikacija specifičnih za potrebe agencije.

3. Rukovodilac Divizije za unutrašnje IKT Sisteme izveštava direktoru Departmana za usluge sajber bezbednosti.

4. Broj zaposlenih u Diviziji za unutrašnje IKT Sisteme je tri (3).

POGLAVLJE III
ZAVRŠNE ODREDBE

Član 17
Završne odredbe

1. Dozvoljen je premeštaj osoblja u skladu sa zakonodavstvom o javnim službenicima unutar institucije, ako se smatra neophodnom za nesmetano odvijanje posla.

2. Povećanje ili smanjenje broja osoblja u skladu sa zakonom o godišnjem budžetu ne stvara potrebu za izmenama i dopunama ove Uredbe, osim u slučajevima kada se uspostavljaju i/ili gase organizacione strukture.

3. U skladu sa stavom 2. ovog člana, odredbe zakona o godišnjem budžetu su sastavni deo ove uredbe.

Član 18
Prilog

Sastavni deo ovog pravilnika je Prilog 1 – Organogram Agencije za sajber bezbednost.

Član 19
Stupanje na snagu

Ova Uredba stupa na snagu na dan objavljivanja u Službenom listu Republike Kosovo.

Albin KURTI

Premijer Republike Kosovo

06 mart 2024

Prilog br. 1:
ORGANOGRAM AGENCIJE ZA SAJBER BEZBEDNOST

ORGANOGRAM AGENCIJE ZA SAJBER BEZBEDNOST			
Struktura	**Klasa**	**Grupa** (opšta i posebna)	**Broj**
1. KANCELARIJA IZVRŠNOG DIREKTORA			**Ukupno 6**
− Izvršni direktor	− Viši rukovodilac 2		1
− Viši službenik za upravljanje operacijama i projektima	− Profesionalni 1	60. Gr. Specijalista za sajber bezbednost	1
− Viši službenik za upravljanje bezbednošću informacija	− Profesionalni 1	60. Gr. Specijalista za sajber bezbednost	1
− Viši razvijač za sajber bezbednost za međunarodnu saradnju	− Profesionalni 1	60. Gr. Specijalista za sajber bezbednost	1
− Viši službenik za informisanje i komunikacije	− Profesionalni 1	10. Gr. Specijalista za informisanje i odnose sa javnošću	1
− Administrativni pomoćnik	− Profesionalni 3	58. Gr. Specijalista opšte uprave	1
2. NACIONALNI CENTAR ZA PREVENCIJU I REAGOVANJE NA SAJBER INCIDENTE			**Ukupno 12**
− Direktor Nacionalnog centra za prevenciju i reagovanje na sajber incidente	− Srednji rukovodilac		1
2.1 Divizija za analizu i prevenciju incidenata			**Ukupno 5**
− Rukovodilac Divizije za analizu i prevenciju incidenata	− Niži rukovodilac		1
− Viši analitičar za sajber bezbednost	− Profesionalni 1	60. Gr. Specijalista za sajber bezbednost	1
− Viši analitičar za procenu slabosti i pretnji	− Profesionalni 1	60. Gr. Specijalista za sajber bezbednost	1
− Viši službenik za pretnje i ranjivost	− Profesionalni 1	60. Gr. Specijalista za sajber bezbednost	2
2.2 Divizija za upravljanje incidentima			**Ukupno 6**
− Rukovodilac Divizije za upravljanje incidentima	− Niži rukovodilac		1
− Viši inženjer sajber bezbednosti	− Profesionalni 1	60. Gr. Specijalista za sajber bezbednost	1
− Viši službenik za reagovanje na incidente	− Profesionalni 1	60. Gr. Specijalista za sajber bezbednost	2
− Viši službenik za sajber forenziku	− Profesionalni 1	60. Gr. Specijalista za sajber bezbednost	2

3. DEPARTMAN ZA STANDARDE I NADZOR − Direktor Departmana za standarde i nadzor	− Srednji rukovodilac		**Ukupno 8** 1
3.1 Divizija za standarde i politiku − Rukovodilac Divizije za standarde i politike − Specijalista za bezbednost informacija − Službenik za politiku i tehničke standarde	− Niži rukovodilac − Profesionalni 1 − Profesionalni 1	 60. Gr. Specijalista za sajber bezbednost 60. Gr. Specijalista za sajber bezbednost	**Ukupno 3** 1 1 1
3.2 Divizija za standarde i politiku − Rukovodilac Divizije za nadzor i praćenje − Inspektor za sajber bezbednost − Razvijač bezbednosti informacionih sistema	− Niži rukovodilac − Profesionalni 1 − Profesionalni 1	 60. Gr. Specijalista za sajber bezbednost 60. Gr. Specijalista za sajber bezbednost	**Ukupno 4** 1 2 1
4. DEPARTMAN ZA USLUGE SAJBER BEZBEDNOSTI Direktor Departmana za usluge sajber Bezbednosti	− Srednji rukovodilac		**Ukupno 12** 1
4.1 Divizija za sertifikaciju opreme i usluga − Rukovodilac Divizije za sertifikaciju opreme i usluga − Specijalista za procenu tehničke podobnosti − Analitičar nepouzdanih proizvoda i usluga	− Niži rukovodilac − Profesionalni 1 − Profesionalni 1	 60. Gr. Specijalista za sajber bezbednost 60. Gr. Specijalista za sajber bezbednost	**Ukupno 3** 1 1 1
4.2 Divizija za tehničke i savetodavne usluge − Rukovodilac Divizije za tehničke i savetodavne usluge − Službenik za odgovore na zahteve i tehničku podršku − Viši razvijač sistema i usluga sajber bezbednosti	− Niži rukovodilac − Profesionalni 1 − Profesionalni 1	 60. Gr. Specijalista za sajber bezbednost 60. Gr. Specijalista za sajber bezbednost	**Ukupno 5** 1 2 2
4.3 Divizija za unutrašnje IKT sisteme − Rukovodilac Divizije za unutrašnje IKT sisteme − Viši administrator mreže i sistema − Viši razvijač softvera i administrator baze podataka	− Niži rukovodilac − Profesionalni 1 − Profesionalni 1	 61. Gr. - Specijalista za IKT sisteme 50. Gr. Specijalista za softver i aplikacije	**Ukupno 3** 1 1 1

ORGANOGRAM AGENCIJE ZA SAJBER BEZBEDNOST