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

Nr. 19/107
Datë: 18.06.2019

Në mbështetje të nenit 92 paragrafi 4. dhe të nenit 93 paragrafi (4) të Kushtetutës së Republikës së Kosovës, duke u bazuar në nenin 4 të Rregullores Nr. 02/2011 për Fushat e Përgjegjësisë Administrative të Zyrës së Kryeministrit dhe Ministrive, e ndryshuar dhe e plotësuar me Rregulloren Nr. 15/2017, me Rregulloren Nr. 16/2017, me Rregulloren Nr. 07/2018, me Rregulloren Nr. 26/2018 dhe me Rregulloren Nr. 30/2018, në pajtim me nenin 19 të Rregullores së Punës së Qeverisë së Republikës së Kosovës Nr. 09/2011, Qeveria e Republikës së Kosovës, në mbledhjen e mbajtur më 18 qershor 2019, nxjerr këtë:

V E N D I M

1. Aprovohet Koncept Dokumenti për Masat e Sigurisë së Rrjeteve të Sistemeve të Informacionit.

2. Obligohet Ministria e Zhvillimit Ekonomik dhe institucionet tjera kompetente për zbatimin e këtij vendimi, në pajtim me Rregulloren e Punës së Qeverisë.

3. Vendimi hyn në fuqi ditën e nënshkrimit.

Ramush HARADINAJ
Kryeministër i Republikës së Kosovës

Iu dërgohet:

- Zëvendëskryeministrave
- të gjitha ministrive (ministrave)
- Sekretarit të Përgjithshëm të ZKM-ës
- Arkivit të Qeverisë

Republika e Kosovës
Republika Kosova-Republic of Kosovo
Qeveria – Vlada - Government
Ministria e Zhvillimit Ekonomik
Ministarstvo Ekonomskog Razvoja-Ministry of Economic Development

Koncept dokument o

Merama bezbednosti mreža i informacionih sistema

Pripremljeno od strane: Ministarstva ekonomskog razvoja – Odeljenje za poštu i telekomunikacije i informacionu komunikacionu tehnologiju

April, 2019.

Sadržaj

Upotrebljene skraćenice

KD – Koncept dokument

MER – Ministarstvo ekonomskog razvoja

GPRV – Godišnji program o radu Vlade

RG – Radna grupa za izradu nacrta KD-a

NPS-SSP - Nacionalni program za sprovođenje Sporazuma o stabilizaciji i pridruživanju

MSP – Mala i srednja preduzeća

CSIRT – Tim za reagovanje na kompjuterske incidente

KSV-KP– Koordinacioni sekretarijat Vlade – Kancelarija premijera

RAEPK – Regulatorni autoritet za elektronske i poštanske komunikacije

AID – Agencija za informaciono društvo

VK – Vlada Kosova

MF – Ministarstvo finansija

MI – Ministarstvo infrastrukture

MUP – Ministarstvo unutrašnjih poslova

MJU – Ministarstvo javne uprave

CBK – Centralna banka Kosova

KOSTT - Operator sistema, prenosa i tržišta

KEDS – Kosovska kompanija za distribuciju i snabdevanje električnom energijom

KEK – Energetska korporacija Kosova

PEU – Provajder esencijalnih usluga

PDU – Provajder digitalnih usluga

EU – Evropska Unija

DPTTIK – Odeljenje za poštu i telekomunikacije i informacionu komunikacionu tehnologiju

ZMIS – Zaštita mreže i informacionih sistema

KII – Kritična informaciona infrastruktura

KI – Kritična infrastruktura

Sažetak koncept dokumenta

Opšte informacije	
Naslov	Koncept dokument o merama bezbednosti mreža i informacionih sistema
Ministarstvo	Ministarstvo ekonomskog razvoja
Kontakt osoba	Fjolla Kozniku – Bajrami; 038 200 21586; e-mail:fjolla.k.bajrami@rks-gov.net
GPRV	Nadovezuje se sa Tabelom B i Ciljem 3 (Stvaranje povoljnog pravnog, regulatornog okruženja, izrada strateških dokumenata i regionalna saradnja u sektoru informacionih komunikacionih tehnologija i poštanskom sektoru), Aktivnost 3.1. Ovaj dokument je takođe deo liste Koncept dokumenata za godine 2018-2019.
Strateški prioritet	Pripremanje ovog KD-a nije specifikovano kao naziv u nekom strateškom dokumentu, već kao oblast koja se treba pokrivati, predviđen je u strateškim ciljevima Nacionalne strategije za kibernetičku bezbednost i Akcionom planu 2016-2020 koji se nadovezuje sa dokumentom o planiranju i izveštavanju prema zahtevima EU-a, planiranih u NPSSSP 2019 Poglavlje 10 – Pokazatelj: 3.10.1 Informaciono društvo i mediji.

Odluka	
Glavno pitanje	Incidenti kibernetičke bezbednosti su u porastu i mogućnost intervenisanja u mrežama i informacionim sistemima kao i široka rasprostranjenost koju mogu imati ovi incidenti, smatrani su jednim od problema koji zahteva hitno rešenje. Ove okolnosti su obavezale preduzimanje mera za zaštitu mreža i informacionih sistema koji se smatraju kritičnom infrastrukturom i kroz koje se pružaju esencijalne i digitalne usluge.

Sažetak konsultacija	Formirana je radna grupa, u kojoj su uključeni predstavnici svih ministarstava koja se povezuju sa delokrugom ovog KD-a, javnih i privatnih kompanija u okviru kojih funkcionišu esencijalne usluge. Radna grupa je izradila nacrt KD-a koji je bio predmet procedura predviđanih uputstvom u priručnikom za izradu KD-a gde su predviđane preliminarne konsultacije, javni sastanak kao i javna diskusija u online platformi. Sve ove procedure su izvršene prema uputstvima i rokovima koji su opisani i u tabeli (slika 7) . Tokom perioda javne konsultacije nije primljen nijedan komentar, primedba ili sugestija bilo u pisanom obliku ili usmeno od strane interesnih strana, institucija uključenih u adresaru za relevantne institucije na osnovu člana 7. i 32. i Pravilnika o radu Vlade Republike Kosovo br. 09/2011, za preliminarno i javno konsultovanje. RG je tokom izrade ovog nacrta, kao jedinu mogućnost dobijanja informacija u vezi sa funkcionisanjem sektora uticanih od strane Direktive EU-a br. 2016/1148 u vezi sa merama za viši nivo bezbednosti mreže i informacionih sistema (poznata kao NIS Direktiva), imala indirektan oblik dobijanja informacija šta je predstavljalo jednu od poteškoća sa kojima je suočena RG tokom izrade ovog nacrta.
Predložena opcija	Poželjna opcija – Izrada novog zakona

Glavni očekivani uticaji	
Budžetski uticaji	Izrada pravnog akta prema ovom KD-u neće imati uticaja na budžet Kosova obzirom da će obaveze nadležnog autoriteta za sprovođenje, nadgledanje i praćenje sprovođenja odredbi koje reguliše NIS Direktiva, a koje transponuje ovaj zakonski akt, obavljati OPTIKT u okviru MER-a.
Ekonomski uticaji	Izrada zakonskog akta, na osnovu ovog KD-a će: - Imati blagi uticaj na porast broja i mogućnosti pronalaženja radnih mesta i pružanju usluga ili proizvoda u određenim sektorima; - Povećati mogućnost povećanja stranih direktnih investicija, promovisanja inovacije i istraživanja kao i konkurentnosti; - Povećati bezbednost u mrežama javnog i privatnog sektora kao što su: transport, zdravstvo, energija, snabdevanje pijaćom vodom, digitalna infrastruktura, infrastruktura bankarskog i finansijskog tržišta i pružaoci digitalnih usluga.
Društveni uticaji	Izrada zakonskog akta na osnovu ovog KD-a će: - Imati blagi uticaj na profesionalno osposobljavanje i prekvalifikaciju. - Stvoriti mogućnosti za sprečavanje i lakše otkrivanje kriminalnih radnji u mrežama i informacionim sistemima, smanjivanje nivoa korupcije i imaće efekat na prava i bezbednost ugroženih žrtava.
Uticaji na životnu sredinu	U ovoj kategoriji ne postoje relevantni uticaji koji se mogu očekivati.
Međusektorski uticaju	Ne postoje relevantni uticaji u ovoj kategoriji
Administrativne takse za kompanije	Izrada zakonskog akta, na osnovu ovog KD-a će povećati troškove privatnih i javnih provajdera esencijalnih i digitalnih usluga tokom pružanja usluga ali u poređenju sa očekivanim koristima, ovi troškovi su minimalni.
Testiranje MSP-ova	Nije primenjen poseban test MSP-a ali nije isključen iz konsultacija.

Naredni koraci	
Kratkoročni	Najvažnije aktivnosti koje se očekuju da će biti razvijene u vremenskom roku u okviru jedne godine nakon usvajanja ovog koncept dokumenta: - Formiranje jedne radne grupe za izradu politika koje regulišu oblast koju određuje ovaj KD; - Organizovanje radionica i sastanaka sa pogođenim stranama; - Angažovanje eksperata (po potrebi).
Srednjoročni	Stvaranje pravnog osnova za: - Identifikaciju usluga i provajdera esencijalnih usluga; - Identifikaciju provajdera digitalnih usluga; - Podizanje kapaciteta i infrastrukture OPTIKT za nadgledanje, praćenje i sprovođenje zakonskog akta koji će transponovati NIS direktivu; Podizanje kapaciteta CERT–a na nivou nacionalnog CSIRT-a koji deluje u okviru jedinice KOS-CERT (RKEPK).

Uvod

Ovim KD-om će se odrediti nadležnosti i obaveze OPTIKT-a za praćenje sprovođenja mera za zaštitu mreža i informacionih sistema za sektore čije će se usluge smatrati esencijalnim kao i Tima CSIRT- a.

U zelenom dokumentu Evropskog programa za zaštitu IK-a, Evropska Komisija je identifikovala Informacionu i Komunikacionu Tehnologiju, kao i jedan od kritičnih sektora, za koji je neophodno povećanje bezbednosnih mera.

Zaštita kritične informacione infrastrukture smatrana je važnim segmentom za bezbednost koja zahteva tretiranje i odgovarajuću pažnju, šta je strateški cilj „Državne strategije za kibernetičku bezbednost i akcioni plan 2016-2019“ ali koji nije planiran u Aktivnostima akcionog plana ove Strategije.

Uprkos tome, MER kao kreator politika u oblasti informacionog društva je zamislila neophodnost preduzimanja bezbednostnih mera za ZMIS koja je smatrana kao KI sa ciljem zaštite provajdera i korisnika esencijalnih usluga i uspostavljanje kredibiliteta u pružanim uslugama koja zavise od strane KII.

U saradnji sa relativnim ministarstvima i interesnim stranama, formirana je Radna grupa odlukom generalnog sekretara MRE-a, br. 02/698, od dana 12.04.2018. godine i dopunjen formularom br.

02/182, od dana 23.01.2019. godine, na zahtev KSV-a, za izradu Koncept dokumenta, sa ciljem adresiranja potreba za zaštitu mreža i informacionih sistema.

Takođe, kroz ovaj KD je predviđeno transponovanje NIS direktive za bezbednost mreža i informacionih sistema, koji je obuhvaćen i u listi Koncept dokumenata za 2018. i 2019. godinu, kao i predlog adekvatnije opcije za tretiranje bezbednosnih mera ZMIS-a.

ZMIS koji je smatran kao KI, imaće uticaja i u drugim sektorima koji pružaju esencijalne usluge, koja u potpunosti zavise od KII, i očekuje se da će imati uticaj na bezbednost PEU-a za zaštitu pružanih usluga.

Stoga, na osnovu uputstva i priručnika za izradu dokumenata, izrađen je ovaj dokument koji će predložiti preporučenu opciju iz radne grupe, zasnovanu na analizi u vezi sa važećim zakonodavstvom za ZMIS.

Slika 1: Tabela sa opštim informacijama o koncept dokumentu

Naslov	Koncept dokument o merama bezbednosti mreža i informacionih sistema
Ministarstvo	Ministarstvo ekonomskog razvoja
Kontakt osoba	Fjolla Kozniku – Bajrami
GPRV	Nadovezuje se sa Tabelom B i Ciljem 3 (Stvaranje povoljnog pravnog, regulatornog okruženja, izrada strateških dokumenata i regionalna saradnja u sektoru informacionih komunikacionih tehnologija i poštanskom sektoru), Aktivnost 3.1. Ovaj dokument je takođe deo liste Koncept dokumenata za godine 2018-2019.
Strateški prioritet	Pripremanje ovog KD-a nije specifikovano kao naziv u nekom strateškom dokumentu, već kao oblast koja se treba pokrivati, predviđen je u strateškim ciljevima Nacionalne strategije za kibernetičku bezbednost i Akcionom planu 2016-2020 koji se nadovezuje sa dokumentom o planiranju i izveštavanju prema zahtevima EU-a, planiranih u NPSSSP 2019 Poglavlje 10 – Informaciono društvo i mediji
Radna grupa	Članovi radne grupe za izradu Koncept dokumenta o „Merama bezbednosnih mreža i informacionih sistema“ Ministarstvo ekonomskog razvoja: Fjolla Kozniku –Bajrami – Visoki službenik za planiranje i projekte – Predsedavajuća Ajshe Jashari – Rukovodilac divizije IKT-a - Zamenica predsedavajućeg Nol Zekolli – Visoki službenik informacionih tehnologija

	Hana Jakupi – Visoki pravni službenik Enver Basha – Rukovodilac Divizije za telekomunikaciju Mendohije Kabashi-Latifi – Visoki službenik za strateško planiranje i koordinaciju politika; Albiona Ismaili – Službenik za budžet Maria Dodaj – Službenik za informisanje Fahrije Qorraj – Visoki službenik za tretiranje i rodnu ravnopravnost Agencije za informaciono društvo: Gani Zogaj – Direktor Odeljenja za bezbednost i centralne operacije Ministarstvo unutrašnjih poslova: Astrit Hulaj – Rukovodilac divizije za upravljanje sistemima i mrežom. Ministarstvo finansija: Zana Radoniqi – Analitičar budžeta Ministarstvo zdravlja: Donika Gjikolli – Visoki administrator IT-a za softverske sisteme Koordinacionu sekretarijat Vlade: Adil Bytyqi – Visoki službenik za koordinaciju politika Operater sistema prenosa i tržišta: Albert Maloku – administrator mreža i sistema Kosovska energetska korporacija: Uran Thaqi - ISO Telekom Kosova: Ehat Qerimi - Službenik Institucije koje se nisu odazvale pozivu generalnog sekretarijata MER-a za imenovanje njihovih predstavnika za RD: RAEPK;MI;lpko; CBK; KEDS;
Dodatne informacije	Nema

Poglavlje 1: Definisanje problema

Nedovoljan nivo bezbednosti u mrežama i informacionim sistemima, posebno onih koji se smatraju kao KI, koji uključuju javne i privatne energetske sektore, zdravstveni sektor, snabdevanje pijaćom vodom, infrastrukturu bankarskog kao i finansijskog tržišta kao i digitalnu infrastrukturu, predstavlja rizik koji može ugroziti njihovo funkcionisanje i imati uticaja u pružanju usluga ili njihovu zloupotrebu a koja može rezultovati značajnim ekonomskim gubitkom, rizikovanjem života i bezbednosti građana.

Uzimajući u obzir da mreže i informacioni sistemi predstavljaju atraktivan cilj za zlonamerne strane, onda i njihova zaštita zahteva poseban i brz tretman, posebno onoga šta se smatra kao „Kritična informaciona infrastruktura", koju treba smatrati fenomenom koji će imati međusektorski uticaj.

Do sada nije bilo nikakvih posebnih preduzimanja od strane institucija ili provajdera esencijalnih ili digitalnih usluga za povećanje ZMIS-a smatra se kao KI, i tom prilikom usluge koje se pružaju preko njih funkcionišu sa visokim rizikom.

Dosadašnji prioriteti odgovornih institucija bile su orijentisane samo na pozitivne inpute koje donosi korišćenje mreža i informacionih sistema i manje u preduzimanju mera i povećanju kapaciteta za stvaranje nivoa bezbednosti sa onima zemalja EU-a.

Identifikacija incidenata i mogućnost njihovog sprečavanja i zaštite predstavlja jedan od glavnih izazova koji mogu ugroziti i Kosovo, šta povećava potrebu za saradnjom i koordinacijom na nacionalnom i regionalnom nivou u ispunjavanju uslova i ispunjavanju bezbednosnih standarda u oblasti mreža i informacionog sistema.

Zbog međusektorskog uticaja kojeg ima, preduzimanje mera za zajednički nivo bezbednosti mreža i informacionih sistema zahteva koordinaciju i sa drugi sektorima, kao: energija, transport, zdravstvo i sektor snabdevanja pijaćom vodom, infrastrukturu bankarskog i finansijskog tržišta kao i digitalnu infrastrukturu.

Opis postojeće politike i zakonskog okvira

Korišćenje IKT-a je smatrano jednim od najmoćnijih i najefikasnijih sredstava za adresiranje značajnih aspekata razvoja ekonomije zemlje, šta predstavlja i misiju MER-a i jedan od glavnih ciljeva i prioriteta Vlade Kosova. Međusektorska pokrivenost i višedimenzionalna upotreba IKT-a omogućile su adresiranje značajnih aspekata ekonomskog razvoja i sveobuhvatnog obuhvatanja društva.
Pored upotrebe i prostiranja mreža i informacionih sistema, jedan od ciljeva trenutne politike je preduzimanje mera za sprečavanje i unapređivanje njihove bezbednosti naspram incidenata i povećanje nivoa njihove bezbednosti na nivou zemalja EU-a.

Podizanje kapaciteta, planiranje, razmenjivanje informacija i koordinacija zajedničkih aktivnosti i zahteva bezbednosti za sve operatere da efikasno odgovore na izazove bezbednosti mreže i informacionih sistema, takođe su zahtev NIS direktive.

Ovo je istovremeno povećalo potrebu za dopunjavanje pravne osnove za povećanje nivoa bezbednosti mreža i informacionih sistema, posebno onih koji se smatraju kritičnom infrastrukturom koja igraju značajnu ulogu u pružanju esencijalnih usluga.

U cilju definisanja mera za povećanje nivoa bezbednosti mreža i informacionih sistema koji se koriste kao kritična infrastruktura, do sada je usvojeno nekoliko strateških i pravnih dokumenata i u toku je pripremanje drugih koji će upotpuniti postojeću ravnu infrastrukturu, što je ujedno i ovaj KD za transponovanje NIS direktive.

Postojeći dokumenti koji se nadovezuju sa koncept dokumentom o bezbednosti mreže i informacionih sistema

Nacionalna strategija za razvoj (2016-2021) – fokusira se na ekonomski rast, čije se sprovođenje smatra sredstvom za podsticanje kosovske agende za evropske integracije.
Stub 4, Mera 30 predviđa da će NSR obezbediti koordinaciju raznih aktera sektora IKT-a kako bi se obezbedila šira rasprostranjenost i upotreba informacione tehnologije u procesima poslovanja, javnih i obrazovnih institucija.

Politike sektora elektronskih komunikacija – Digitalna agenda za Kosovo 2013-2020 – U okviru Prioriteta 1: „Razvoj infrastrukture IKT-a“ , i drugog cilja: „postizanje bezbednosti i integriteta mreža i usluga elektronskih komunikacija“, predviđen je kao zadatak i primenjivanje mera bezbednosti, upravljanje rizikom, kontrole incidenata mreža elektronskih komunikacija, informacioni sistemi sa ciljem postizanja bezbednosti i pouzdanosti informacioni sistema javnih sektora i nacionalne infrastrukture kritičnih informacija sa ciljem povećanja javnog i poslovnog poverenja u kibernetičkom prostoru.

Državna strategija za kibernetičku bezbednost i akcioni plan 2016 - 2020 – dokument koji predstavlja viziju Vlade Kosova za kibernetičku bezbednost i relativni akcioni plan. Državna strategija za kibernetičku bezbednost je deo Programa Vlade 2015-2018, kao i nadovezuje se sa Nacionalnim planom za sprovođenje Sporazuma o stabilizaciji i pridruživanju.
Ova strategija ima za cilj adresiranje pitanja kibernetičke bezbednosti u Republici Kosovo, za čije su postizanje određeni strateški objektivi i konkretne aktivnosti politika koja se trebaju sprovoditi. Strateški ciljevi ove strategije su:

1. Zaštita kritične informacione infrastrukture;
2. Institucionalni razvoj i podizanje kapaciteta;
3. Izgradnja javno-privatnog partnerstva;
4. Reakcija na incidente i
5. Međunarodna saradnja

Zakon o sprečavanju i suzbijanju kibernetičkog kriminala – ima za cilj sprečavanje i suzbijanje kibernetičkog kriminala konkretnim merama, sprečavanje, otkrivanje i sankcionisanje prekršaja kroz kompjuterske sisteme, obezbeđujući poštovanje ljudskih prava i zaštitu ličnih podataka.

Nacionalni plan za sprovođenje Sporazuma o stabilizaciji i pridruživanju (NPSSSP) 2017 – 2021- u okviru Bloka 3: EVROPSKI STANDARDI – USKLAĐIVANJE KOSOVSKOG ZAKONODAVSTVA SA ACQUIS-OM EU-a, poglavlje 10 acquis-a: Informaciono društvo i mediji preuzima odgovornost za sprovođenje člana 111 – Poglavlje VIII SSP-a, koji se odnosi na mrežu i usluge elektronskih komunikacija.

Godišnji plan rada Vlade Kosova za 2018. godinu – ovim planom je određena izrada Koncept dokumenta o „Merama bezbednosti mreža i informacionih sistema" u vremenskom periodu do decembra 2018. godine. Obzirom da se nije uspelo da se ovaj KD usvoji prema planiranju, prenesen je u GPRV 2019, vremenski rok mart. Ovaj KD je uključen i u listi Koncept dokumenata za 2018. i 2019. godinu.

Zakon br. 04/l-094 o uslugama informacionog društva (SL/Br. 6, datum: 11. april 2012. godine) - reguliše aktivnost usluga informacionog društva, jedan od ciljeva ovog zakona je smanjenje potencijalnih problema zloupotreba tokom elektronskih transakcija i adresiranje bezbednosti informacionih sistema.

Zakon br. 06/L-014 o kritičnoj infrastrukturi (SL/Br. 5 / 27. APRIL 2018) – reguliše nacionalnu kritičnu infrastrukturu i pruža uputstva za identifikaciju infrastruktura koja će se odrediti kao evropska kritična infrastruktura. Ovaj zakon takođe identifikuje sektore i kriterijume nacionalne i evropske kritične infrastrukture i pruža uputstva za njihovo upravljanje, uključujući analizu rizika, karakteristike planova bezbednosti za vlasnike/operatere, uloge i odgovornosti koordinatora bezbednosti kritične infrastrukture, kao i novčane kazne za neizvršenje.

Politički dokument, zakon ili podzakonski akt	Veza sa politikom ili planskim dokumentom kroz internet ili zakonskim aktima u Službenom listu	Državna (e) institucija (e) odgovorna (e) za sprovođenje	Uloga i obaveze institucije (a)
Nacionalna strategija za razvoj (2016-2021)	http://www.kryeministri-ks.net/repository/docs/Strategjia_Kombetare_per_Zhvillim_2016-2021_Shqip.pdf	VK – Resorna ministarstva	Stub 4, Mera 30 predviđa da će NSR obezbediti koordinaciju raznih aktera sektora IKT-a kako bi se obezbedila šira rasprostranjenost i upotreba informacione tehnologije u procesima poslovanja, javnih i obrazovnih institucija.

Nacionalna strategija za kibernetičku bezbednost i akcioni plan 2016 - 2020	http://www.kryeministri-ks.net/repository/docs/Strategjia_Shteterore_per_Sigurine_Kibernetike_dhe_Plani_i_Veprimit_2016-2019_per_publikim_1202.pdf	MUP, MER, MJU, RAEPK, MI, MTI	Razvoj infrastrukture IKT-a, podizanje nivoa kibernetičke bezbednosti
Zakon o sprečavanju i suzbijanju kibernetičkog kriminala	http://mzhe-ks.net/repository/docs/LIGJIPERPARANDALIMINDHE_LUFTIMINE_KRIMITKIBERNETIKE2010166-alb.pdf	MUP, MJU, MER, RAEPK, MI, MTI	Sprečavanje i suzbijanje kibernetičkog kriminala konkretnim merama
Zakon br. 04/l-094 o uslugama informacionog društva (SL/ Br. 6, datum: 11. april 2012. godine)	https://gzk.rks-gov.net/ActDetail.aspx?ActID=2811	AID (MJU), MER, MTI	Smanjenje potencijalnih problema zloupotreba tokom elektronskih transakcija i adresiranje bezbednosti informacionih sistema.
Zakon br. 06/L-014 o kritičnoj infrastrukturi (SL / Br. 5 / 27. APRIL 2018. godine)	https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=16313	MUP	Identifikacija kritične nacionalne i evropske infrastrukture

Slika 2:Relevantni politički dokumenti, zakoni i podzakonski akti

Problem, uzroci i zainteresovane strane

Ubrzani razvoj i korišćenje interneta, mreža i informacionih sistema uticao je pozitivno na poboljšanje kvaliteta i povećanje brzine usluga, povećanje produktivnosti i unapređenje životnog standarda. Ovo je povećalo mogućnosti njihove izloženosti prema napadima i incidentima, šta predstavlja veliku pretnju za njihovo funkcionisanje.

Uprkos sveukupnoj upotrebi infrastrukture TIK-a, do sada nisu tretirani na adekvatan i dovoljan način rizici koji su u porastu, koji predstavljaju prednju po bezbednosti sistema i informacionih mreža i uticaje koje mogu imati na njihovu upotrebu i zloupotrebu.

Zbog fragmentiranog dosadašnjeg pristupa bezbednosnih problema informacionog društva i nedovoljne koordinacije odgovornih institucija koje tretiraju ove probleme kao i nedostatka pritiska od strane PEU-a i PDU-a, do sada je bilo stagnacije u tretiranju problema bezbednosti mreža i informacionih sistema.

Uzimajući u obzir rizike koji se mogu desiti kao i uticaje koje mogu imati u mreži i informacionim sistemima, Vlada Republike Kosovo je izradila Državnu strategiju za kibernetičku bezbednost i akcioni plan 2016 – 2019 koji je jedan od osnovnih ispunjenih uslova za transponovanje NIS direktive.

Takođe, zakon o kritičnoj infrastrukturi se ograničava u identifikaciji i određivanju kritičnih infrastruktura i obavezivanju operatera ove infrastrukture za izradu i dostavljanje plana bezbednosti.
Ovaj plan podrazumeva uključivanje mera za sprečavanje i zaštitu od incidenata i mrežne infrastrukture i sistema definisanih kao kritična infrastruktura, koja su odgovornost OPTIKT-a kao kreator politika u okviru MER-a.
Posebno tretiranje problema i neophodnih mera za podizanje nivoa bezbednosti ovih mreža i sistema treba da pokriva minimalne uslove planiranja i podizanja tehničkih i ljudskih kapaciteta, razmenjivanja informacija i saradnje u vezi sa zajedničkim bezbednosnim zahtevima za PEU i PDU.
Odgovor na globalne i nacionalne zahteve za tretiranje bezbednosti mreža i informacionih sistema povećala je potrebu i neophodnost bolje koordinacije između institucija kao pogođene strane. Ove institucije na direktan način tretiraju probleme za podizanje bezbednosnih mera u KII PEU-a i PDU-a u sektoru energetike, transporta, zdravstva, snabdevanja pijaćom vodom, infrastrukturi bankarskog i finansijskog tržišta i digitalnoj infrastrukturi.

Strane koje se na direktan ili indirektan način nadovezuju sa problemima bezbednosti mreže i informacionih sistema su:

Ministarstvo ekonomskog razvoja kroz OPTIKT – predlaže, izrađuje i obezbeđuje sprovođenje političkih dokumenata i strategija elektronskih komunikacija i informacionog društva. Takođe, između ostalih obaveza i odgovornosti OPTIKT-a u oblasti informacionog društva je podrška informacione tehnologije i inovacija, obezbeđivanje kvaliteta usluga i tehničkih standarda u oblasti telekomunikacija, kreiranje politika za promovisanje konkurentnosti u oblasti telekomunikacija, razmatranje potreba i zahteva potrošača u oblasti telekomunikacija, podrška pristupa tehnologiji za sve građane Kosova i podsticanje razvoja sistema osposobljavanja u informacionim tehnologijama.

Ministarstvo unutrašnjih poslova – ima glavnu ulogu u koordinaciji strategije, praćenju sprovođenja Akcionog plana kao i izradu periodičnih izveštaja. MUP je takođe odgovoran za izradu i praćenje politika i zakonodavstva u oblasti opšte i kibernetičke bezbednosti. Policija Kosova je u koordinaciji sa MUP-om, snosi glavnu odgovornost u suzbijanju kibernetičkog kriminala, kroz Sektor za kibernetički kriminal i ostale potporne strukture u okviru Policije Kosova.

Policija Kosova će takođe poslužiti i kao stalna kontakt tačka 24/7 za međunarodnu saradnju u oblasti kibernetičkog kriminala.

Agencija za informaciono društvo – koordiniše, rukovodi i nadgleda procese i mehanizme elektronskog upravljanja u vezi sa infrastrukturom IKT-a, proširenjem internet usluga i internet sadržaja u institucijama Republike Kosovo, akumulaciju, administraciju, proširenje i očuvanje podataka, uspostavljajući Državni centar elektronskih podataka kao i Bezbednost i zaštitu

elektronske komunikacione infrastrukture. AID, po potrebi, pomaže relevantnim institucijama u suzbijanju kibernetičkog kriminala i pruža zaštitu ličnih podataka u elektronskom obliku, u skladu sa važećim zakonodavstvom.

Regulatorni autoritet za elektronsku i poštansku komunikaciju – je regulatorni organ, koji sprovodi i prati regulatorni okvir koji je određen Zakonom o elektronskim komunikacijama, Zakonom o poštanskim uslugama, kao i politikama razvoja komunikacione oblasti i poštanskih usluga.

Glavni problem, uzroci i efekti

Slika 3: Stablo problema

Efekti

1. Ugrožavanje integriteta, privatnosti i života pojedinca.
2. Individualni ili institucionalni finansijski gubitak
3. Zloupotreba podataka u informacionim sistemima

Glavni problem

- Nizak nivo bezbednosti mreža i informacionih sistema koji se koriste kao kritična infrastruktura.

Uzroci

1. Postojeći pravni okvir je nepotpun i ne tretira adekvatno bezbednost mreža i informacionih sistema korišćenih kao kritična infrastruktura
2. Nedostatak mera bezbednosti za mreže i informacione sisteme korišćene kao kritična infrastruktura unutar samih operatera koji pružaju esencijalne i digitalne usluge.

Slika 4: Pregled zainteresovanih strana na osnovu definicije problema

Naziv zainteresovane strane	Uzrok-ci sa kojima je povezana strana	Uzrok-ci sa kojima je povezana strana	Način na koji je strana povezana sa ovim uzrokom (uzrocima) ili efektom (efektima)
MER	1	/	MER kao odgovoran za stvaranje pravne infrastrukture za oblast informacionog društva do sada nije ispunila pravnu osnovu za podizanje nivoa mreža i informacionih sistema
MD	2	3	Nedostaje bezbednost u upravljanju zdravstvenih podataka koji se čuvaju i arhiviraju elektronski, u sistemu zdravstvene informacije

MI	/	1,3	Nedostaje bezbednost u upravljanju kritičnom infrastrukturom informacije u oblasti transporta
MUP	/	1,3	Izdao je zakon o nacionalnoj i evropskoj kritičnoj infrastrukturi, ali ovaj zakon ne pokriva mere bezbednosti za kritičnu infrastrukturu mreža i informacionog sistema
Operateri esencijalnih usluga	2	1,2,3	Do sada ne postoji lista ovih operatera koji upravljaju i pružaju mreže esencijalnih usluga.
Provajderi digitalnih usluga	2	1,2,3	Do sada ne postoji lista ovih esencijalnih usluga.
RAEPK	1	3	Jedinica KOS-CERT u okviru ove institucije ima ograničene kapacitete za osiguranje sprečavanja i identifikacije mogućih napada na mreže i informacionim sistemima.
MJU	/	2	Upravlja i obezbeđuje centralnu informacionu mrežu vladinih institucija

Poglavlje 2: Ciljevi

Uz transponovanje odredbi NIS Direktive cilja se podizanje nivoa opšte bezbednosti i fleksibilnosti mreže i informacionih sistema i posebno onih koji se koriste kao KI na nivou sa onima u zemljama EU-a, čije će sprovođenje omogućiti uspostavljanje mehanizama za podizanje tehničkih i profesionalnih kapaciteta.

Kroz ovaj KD cilja se kreiranje jednog zakona, čiji je cilj podizanje nivoa bezbednosti mreže i informacionih sistema i povećanje njihove otpornosti i elastičnosti prema mogućim napadima na nacionalnom i globalnom nivou.

Odredbe ovog zakona će se primenjivati na mrežu i informacioni sistem koji se koristi kao KI u sektoru energetike, transporta, zdravstva, snabdevanja pijaćom vodom, infrastrukturi bankarskog i finansijskog tržišta i digitalnoj infrastrukturi i imaju za cilj podizane nivoa bezbednosti pružanja esencijalnih usluga ovih sektora. Ove mreže i informacioni sistemi ovih sektora treba da se identifikuju kao kritična infrastruktura koja se koristi za pružanje esencijalnih usluga.

Za postizanje gore navedenog cilja predviđeni su sledeći ciljevi:

Cilj 1 – Poboljšanje kapaciteta bezbednosti na nacionalnom nivou za oblast bezbednosti mreža i informacionih sistema korišćenih kao kritična infrastruktura.

Cilj 2 – Povećanje saradnje sa zemljama EU-a i drugim zemljama koje sprovode NIS Direktivu.

Cilj 3 – Bezbednosne mere za upravljanje rizikom i obaveze PEU-a i PED-a za izveštavanje incidenata.

Slika 5: Relevantni ciljevi Vlade

Relevantni cilj	**Naziv relevantnog planskog dokumenta (izvor)**
Zaštita kritične informacione infrastrukture;	Državna strategija za kibernetičku bezbednost i akcioni plan 2016-2019.
Institucionalni razvoj i podizanje kapaciteta;	Državna strategija za kibernetičku bezbednost i akcioni plan 2016-2019.
Međunarodna saradnja	Državna strategija za kibernetičku bezbednost i akcioni plan 2016-2019.

Poglavlje 3: Opcije

Ne-dopunjavanje pravnog okvira može se smatrati jednim od razloga za nedovoljno tretiranje bezbednosti mreže i informacionih sistema, posebno onaj koji je identifikovan kao KI.

Za popunjavanje ovog jaza i dopune postojećeg pravnog okvira predviđena je izrada ovog KD koji će prethoditi izdavanju zakona koji uređuje oblast bezbednosti mreže i informacionih sistema i koji je uređen sa Direktivom o NIS-u. Analizirani su uticaji koji mogu nastati transponiranjem ove direktive u domaćem zakonodavstvo na osnovu kojih su identifikovane nekoliko opcije koje se mogu koristiti.

Identifikovane opcije su sledeće:

3.1. Opcija 1 - Održavanje stanja u status quo (bez promene)

Do sada, Kosovo nije bilo izloženo napadima i opasnostima istaknutih u svojoj mreži zbog ograničenih usluga koje se pružaju preko ove mreže. Međutim, to ne podrazumeva i nastavak ove bezbednosnog stanja zbog brzog razvoja i integracije nacionalne mreže u globalnu mrežu.

Postojeće zakonodavstvo i, na kraju i Zakon o kritičnoj infrastrukturi ne tretiraju bezbednosne mere mreže i informacionih sistema korišćeni kao kritična infrastruktura.

Stoga, održavanje ovog stanja tj. ne izdavanje bilo kojeg dotičnog pravnog akta, poveća će negativan uticaj na PEU-e, institucije i pojedince koji koriste pružene usluge i gubitak njihovog poverenja za korišćenje ovih usluga.

Svako kašnjenje u transponiranju Direktive o NIS-u će stvoriti prepreke za PEU-e i PDU-e u planiranju bezbednosnih mera za njihovu kritičnu infrastrukturu. To podrazumeva i nastavak negativnog uticaja na e-ekonomiju, e-usluge, rast nepoverenja i nesigurnost korisnika esencijalnih usluga u pruženim uslugama.

Opcija status quo istovremeno će podrazumevati i kašnjenje u ispunjenju obećanja i obaveza institucija Kosova za usklađivanje zakonodavstva sa zakonodavstvom EU u okviru oblasti informacionog društva.

3.2. Opcija 2 - Poboljšanje sprovođenja i izvršenja (Promena postojeće politike - izdavanje pravnog akta o merama bezbednosti mreže i informacionim sistemima)

Izdavanje zakona o uređivanju mere bezbednosti mreže i informacionih sistema korišćeni kao kritična infrastruktura, uređivaće pitanje bezbednosti kompanija koje pružaju esencijalne ili digitalne usluge. Istovremeno bi se ispunili i trenutni zahtevi za dopunu nacionalnog zakonodavstva a istovremeno bi uređivao i ovaj segment bezbednosti.

Poboljšanje postojećeg stanja kroz izdavanje zakona se predviđa da će se postići uspostavljanjem jasnih obavezujućih i nadzornih kriterija za PEU i PDU u podizanju bezbednosnih mera i kapaciteta mreže nacionalnog CSIRT-a.

Nadzor sprovođenja ovog zakona koji se predviđa ovim KD-om će učiniti da DPTTIK koji deluje u okviru MER-a koji će funkcionirati kao tačka kontakta i imaće ulogu Nacionalnog autoriteta kao što je definirano u Direktivi o NIS-u.

Šta će sadržati ovaj zakon?

Ovaj zakon će sadržati sve potrebne odredbe koje će omogućiti transponiranje i prilagođavanje Direktive o NIS-u uslovima Kosova.

- DPTTIK će pratiti i koordinirati aktivnosti o merama bezbednosti mreža i informacionim sistemima korišćene kao kritična infrastruktura za privatni i javni sektor pomenute u Prilogu II Direktive o NIS-u:
- Energetika (električna energija, nafta i gas);
- (Vazdušni, železnički i kopneni) transport;
- Bankarski sistem (kreditne institucije);

- Infrastruktura finansijskog tržišta (operatori trgovačkih objekata i glavne zainteresovane strane);
- Zdravstvo (provajder zdravstvenih usluga - bolnice i klinike);
- Snabdevanje i distribucija vode za piće (snabdevači i distributeri vode namenjeno za ljudsku potrošnju);
- Digitalna infrastruktura (provajderi usluga imena domena DNS, tačke za razmenu interneta IXP i registri imena na čelu domena TLD) kao i usluge pomenute u Prilogu III ove direktive:
- online tržište;
- onlajn pretraživači i
- cloud usluge.

DPTTIK će nadgledati ispunjavanje zadataka vezanih za bezbednost mreža i informacionih sistema PEU-a i PDU-a a istovremeno će služiti i kao "jedina tačka kontakta" koja će imati funkciju povezivanja za osiguranje saradnje sa mrežom CSIRT-a.
DPTTIK je odgovoran za:

- praćenje sprovođenja zakona koji će transponirati Direktivu o NIS-u;
- praćenje sprovođenja kriterijuma za identifikaciju operatera esencijalnih usluga;
- identifikacija usluga koje treba smatrati esencijalnim za održavanje društvenih i ekonomskih kritičnih aktivnosti;
- stvaranje i ažuriranje spiska operatera koji pružaju esencijalne usluge i usluge koje se smatraju esencijalnim i
- nadgledanje PEU-a i PDU-a ukoliko ispunjavaju kriterije bezbednosti za koje su identifikovani.

- "Provajderi esencijalnih usluga" pružaju usluge koje su esencijalne (ključne) za održavanje kritičnih društvenih i/ili ekonomskih aktivnosti, čije pružanje zavisi od mreže i informacionih sistema i obavezni su da:

- pružaju opis mreže i informacionih sistema koje koriste;
- preduzmu odgovarajuće i proporcionalne tehničke i organizacione mere za upravljanje rizicima za bezbednost mreže i informacionih sistema koje se koriste;
- obaveste DPTTIK o incidentima koji imaju veliki uticaj na esencijalne usluge koje one pružaju;
- sprečavaju i minimiziraju uticaj incidenata i
- organizuju godišnju reviziju svojih troškova.

Ovi pružaoci esencijalnih usluga imaju važnu ulogu u pružanju bezbednosti ovih usluga u sektoru zdravstvene infrastrukture, transporta, energije, snabdevanje pijaćom vodom, bankarskoj i finansijskoj infrastrukturi kao i digitalnoj infrastrukturi.
Za klasifikaciju incidenta, treba uzeti u obzir efekte razdvajanja i međusektorske faktore kao što su:

- broj korisnika koji se oslanjaju na pruženu uslugu;
- zavisnost sektora navedenih u Direktivi o NIS;
- uticaj koji može imati u smislu prostiranja i trajanja ekonomskih i društvenih aktivnosti ili u javnoj bezbednosti;

- tržišno učešće PEU-a;
- geografsko prostiranje vezano za zone koje mogu biti pogođene incidentom i
- važnost koju ima PEU za održavanje značajnog nivoa usluga, s obzirom na dostupnost alternativnih sredstava za pružanje te usluge.

- Provajderi digitalnih usluga treba da identifikuju rizike koje se pojave u mreži i informacionim sistemima korišćeni kao kritična infrastruktura i da preduzmu tehničke i organizacione mere, prilagodne i proporcionalne za upravljanje pružanja usluga navedenih u prilogu III Direktive o NIS-u (onlajn tržište, onlajn pretraživači i cloud servis)
  Ovi provajderi digitalnih usluga treba da pružaju odgovarajući nivo bezbednosti za mrežu i informacione sisteme i da uzmu u obzir:
  - bezbednost sistema i objekata;
  - tretiranje incidenata;
  - upravljanje kontinuiteta poslovanja;
  - praćenje, reviziju i testiranje kao i
  - usklađenost sa međunarodnim standardima.

- Mreža reagovanja na incidente bezbednosti - CSIRT će delovati unutar jedinice KOS-CERT-a RAEPK-a u skladu sa zahtevima navedenim u tački 1. priloga I. i pokrivaće najmanje sektore navedene u Prilogu II. i navedene usluge u Prilogu III. Direktive o NIS-u kao i da je odgovoran za tretiranje rizika i incidenta. Ovaj CSIRT će biti ojačan odgovarajućim i dovoljnim kapacitetom za izvršavanje zadataka navedenih u tački 2. Priloga I. Direktive o NIS-u.
  CSIRT će biti odgovoran za:
  - praćenje incidenata na nacionalnom nivou;
  - upozoravanje, uzbunjivanje, obaveštavanje i širenje informacija kod odgovarajućih zainteresovanih strana o rizicima i incidentima;
  - odgovaranje na incidente;
  - vršenje analiza u nastavku rizika i incidenata kao i podizanje svesti o nastaloj situaciji i,
  - učešće u mreži CSIRT-ova.

- Saradnja sa državama članicama sa drugim zemljama koje sprovode Direktivu o NIS-u za podršku i olakšavanje strateške saradnje i razmene informacija i za uspostavljanje međusobnog poverenja (član 1, tačka 2. Direktive o NIS-u)

- Administrativne mere prema PEU-ima i PDU-ima utvrđuju se od DPTTIK-a u slučaju utvrđivanja kršenja ili neispunjavanja dužnosti definisanih ovim zakonom, tokom vršenja njihove delatnosti kao i postupci za žalbu.

3.3. Treća opcija - Promena postojećeg pristupa sprovođenja

Održavanje sadašnje politike i promena samo postojećeg pristupa sprovođenja kroz jačanje DPTTIK-a i jedinice KOS-CERT-a bez uređivanja dužnosti i obaveza u odnosu na PEU-e i PDU-e i obrnuto, nije moguće da se ostvari bez pravne odgovarajuće osnove utvrđene od Direktive o NIS-u.

Bilo koje osnaživanje postojećih mehanizama ne bi moglo da obavezuje sektore koji imaju KI mreža i informacionih sistema da preduzimaju mere za povećanje nivoa bezbednosti svojih mreža i za identifikaciju njihovih esencijalnih usluga sa sadašnjom pravnom osnovom.

Zakon o kritičnoj infrastrukturi tretira opšte načine i kriterije za identifikaciju KI kao i sektore, ali ne navodi mere bezbednosti za kritičnu infrastrukturu određenog sektora.

Stoga, svako moguće tumačenje ovog zakona, sa ciljem povećanja nivoa bezbednosti za sektorsku kritičnu infrastrukturu, ne može se vršiti bez deformacije opšteg cilja i principa za koju je izdata i koja se može smatrati najgora opcija.

Poglavlje 4: Identifikacija i procena budućih uticaja

Na osnovu analize, donji uticaji važe generalno i za opciju 2: Poboljšanje sprovođenja i izvršenja, dok opcije 1. i 3. ne odražavaju uticaje navedene na sl. 6.

Slika 6: Najvažniji uticaji identifikovani za kategoriju uticaja

Kategorija uticaja	**Identifikovani odgovarajući uticaji**
Ekonomski uticaji	Zapošljavanje dodatnog osoblja i prekvalifikacija postojećeg osoblja za PEU-e i PDU-e kao i operativni troškovi za pružanje esencijalnih usluga uticaće na povećanje troškova ovih operatera, što predstavlja značajan trošak za njihovo poslovanje. Operativni troškovi za ova poslovanja obuhvataju rashode za dodatne troškove bezbednosti, administrativne troškove vezane za prijavljivanje incidenata i obezbeđivanje dokaza o proceni rizika sigurnosti ili revizije od strane ovlašćene revizorske kompanije. Ovo će takođe uticati i na povećanje cena esencijalnih usluga i povećanje plaćanja potrošača za korišćenje ovih usluga. Pored toga, povećanje pouzdanosti i bezbednosti mreže i usluge informacije će imati značajan uticaj i predviđa se da će doneti pozitivne uticaje kroz stvaranje povoljnih uslova za strane direktne investicije. Mogući finansijski gubici mogli bi se smanjiti pružanjem sigurnih usluga i to bi poboljšalo poverenje potrošača u digitalnim uslugama, što bi stvorilo nove mogućnosti za poslovanje i digitalnu ekonomiju. Korisnici bi se osećali sigurniji u korišćenju online usluga i to bi poboljšalo njihovo poverenje u online usluge koje pozitivno utiču na domaće tržište. Promovisanje kulture upravljanja rizicima takođe bi podsticao zahtev za izbor sigurnijih proizvoda ITK-a. To bi stvorilo nove mogućnosti i tržišta na Kosovu, kao i stvorilo bi kapitalizaciju istraživačkih investicija kroz poboljšanje komercijalnog korišćenja tih proizvoda. Imajući sigurne platforme za elektronsku trgovinu i druge usluge zasnovane na online platformi mogle bi doneti značajne ekonomske koristi i omogućiće širok krug kompanija da donesu nove proizvode i usluge na tržištu.

Socijalni uticaji	Izrada pravnog akta zasnovanog na ovom KD-u će: - imati blagi uticaj na povećanje broja radnih mesta i na visini plaćanja za sektor bezbednosti koji se razmatra u ovom KD-u; - imati blagi uticaj na povećanje cena esencijalnih usluga; - povećati zahteve PEU-a i PDU-a za stručno osoblje koje zahteva stalno obučavanje i osposobljavanje.
Uticaji na životnu sredinu	Ne očekuje se da će sprovođenje ovog KD-a imati bilo kakav uticaj na životnu sredinu.
Uticaji na osnovna prava	Podiže stepen bezbednosti od napada (zloupotrebe) bezbednosti informacija
Uticaj na rod	Ne očekuje se da će sprovođenje ovog KD-s imati direktan uticaj na rod za dotičan sektor za koje se očekuje da budu regulisani, dodaju se obaveze i zahtevi za kvalifikovanim osobljem u određenoj oblasti bezbednosti mreža i informacionih sistema bez rodne predrasude.
Uticaji socijalne jednakosti	Sprovođenje ovog KD-a može imati indirektni uticaj na socijalnu jednakost, s obzirom da viši nivo bezbednosti mreža i informacionih sistema bi povećao poverenje građana u online usluge, tako da korisnici pružanih usluga putem ove mreže mogu imati više koristi od digitalne mreže (npr. elektronske zdravstvene usluge, transporta, finansija i druge esencijalne usluge).
Uticaj na mlade	Očekuje se da sprovođenje ovog KD-a će imati uticaj na mlade u jačanju poverenja za razvoj inovacije i istraživanja tako da ove ideje budu korišćene za stalni rast nivoa bezbednosti u esencijalnim i digitalnim uslugama koje se pružaju putem mreža i informacionih sistema.
Uticaji na administrativno opterećenje	Sprovođenje ovog KD-a se očekuje da će imati blage uticaje u smislu povećanja administrativnog opterećenja.
Uticaj MSP-a	Ne očekuje se da će sprovođenje ovog KD-a imati uticaj na MSP-oe.

Neki poznati slučajevi napada na informacione mreže

Zbog nedostataka zvanične statistike na nivou Kosova o broju incidenata, njihovom stepenu i uticaju analizirana je statistika EU-a, u cilju što jasnije slike o posledicama koje mogu nastati usled nemara u preduzimanju mera bezbednosti u informacionim mrežama.

Iz statistike EU-a, više od jedne osobe na deset osobe su žrtve prevare preko interneta. Eurobarometar za 2012. godinu za kibernetičku bezbednost je utvrdio da 38% korisnika interneta u EU-u su bili zabrinuti zbog sigurnosti online plaćanja i promenili su svoje ponašanje zbog

zabrinutosti u sigurnosnim pitanjima ili 18% manje su bili zainteresovani za online kupovinu proizvoda i 15% manje koriste e- banking.

Ovaj problem je zahvatio sve delove društva i ekonomije (lokalnu i nacionalnu administraciju, biznis i potrošače), a posebno brojne sektore koji igraju ključnu ulogu u pružanju esencijalnih usluga podrške našoj ekonomiji i društvu. Ovi sektori uključuju energiju, transport, bankarski sistem, infrastrukturu finansijskog tržišta, zdravstvo, snabdevanje i distribuciju pitke vode kao i digitalnu infrastrukturu i provajdere ključnih internet usluga.

Jedan od slučajeva je i kibernetički napad iz 2007. godine u Estoniji, koji je imao negativan uticaj ne samo na pružanje online usluga kao što su e-vlada i e-bankarstvo već je sprečio i korišćenje usluga interneta od građana i preko granica.

Drugi slučaj je kibernetički napad na elektroenergetsku mrežu u Ukrajini 23. decembra 2015. godine. Tri elektro-distributivne kompanije pretrpele su sofisticirani kibernetički napad koji je ishodilo prekidom električne energije za 225.000 ljudi za više od šest sati u pogođenim područjima. Uprkos činjenici da napad nije dugo trajao, kontrolni centri su ostali neaktivni više od dva meseca.

To pokazuje da mreže i informacioni sistemi su međusobno povezani i da svaki incident čak i na lokalnom nivou, može se lako proširiti.

Ovakav efekat snosi rizik da incidenti u mrežama i informacionim sistemima budu distribuirane unutar ili između administracija, što može kompromitovati ili paralizovati većinu područja lokalnih i nacionalnih javnih aktivnosti.

Poglavlje 4.1: Izazovi sa prikupljanjem podataka

Pošto ovaj sektor bezbednosti još nije bio ranije regulisan, nismo imali statističke podatke o mogućim incidentima na bezbednost mreže i informacionih sistema, tako da ovo je bio izazov koji je pratio ceo period pripreme ovog KD. U početku su analizirani svi postojeći strateški dokumenti i zakoni koji se bave pitanjima koja regulišu mreže i informacione sisteme kako bi se prikupili i odabrali podaci o pitanjima koja su razmatrana i ona koja do sada nisu razmatrana.

Shodno tome, primećeno je da osim u bankarski sektor u svim drugim sektorima nedostaju potrebne i dovoljne mere za bezbednost mreža i informacionih sistema, štaviše, neki od tih sektora su u početnoj fazi digitalizacije usluga njihovih mreža.

Treba istaći da poseban izazov za izradu ovog KD-a je bio nedostatak zvaničnih statističkih podataka o broju incidenata i efektima proširenja na nivou Kosova.

Poglavlje 5: Komunikacija i konsultacije

Na pojedinačnim sastancima sa nadležnim osobama sektora obuhvaćenih ovom Direktivom koji su deo RG za izradu ovog KD, raspravljano je o nedostatku preduzimanja mera za podizanje i održavanje nivoa bezbednosti njihovih mreža a izražena je spremnost da njihova podrška neće nedostajati.

Nakon konsolidacije KD-a za mere bezbednosti mreža i informacionih sistema prosledili smo nacrt sa preliminarnu konsultaciju gde su uključene institucije od adresara za dotične institucije za preliminarnu konsultaciju prema članu 7. Poslovnika o radu Vlade 09/2011 kao i stranke pod uticajem koje nisu bile deo radne grupe. Pošto nismo primili nikakav komentar tokom roka za ove konsultacije, smatrali smo da je razumno pozvati strane na javni sastanak kako bismo otvorili raspravu vezano za ovaj KD. Prema uputstvu i priručnika za izradu nacrta KD-a, ovaj nacrt je takođe objavljen i u online platformi za javnu raspravu.

Slika 7: Sažetak aktivnosti komunikacije i konsultacija vršenih za koncept dokument

Proces konsultacija ima za cilj:						
Glavni cilj	Ciljana grupa	Aktivnost	Komuniciranje/ obaveštenje	Vremenski rok	Potreban budžet	Odgovorno lice
Preliminarne konsultacije sa odgovarajućim institucijama, prema članu 7. Poslovnika o radu Vlade 09/2011	MF MEI KP (KSV, KSP, KPP, KJK) MUP MJU RAEPK	Slanje nacrta koncept dokumenta odgovarajućim institucijama za unutrašnju konsultaciju	Preko elektronske pošte	31.10.2018 - 21.11.2018		Fjolla Kozniku Bajrami

Rasprava sa stranama pod uticajem o sadržaju nacrt-koncept dokumenta	Stranke pod uticajem: MZ, MI, MUP, Operateri esencijalnih usluga, provajderi digitalnih usluga, RAEPK, MJU	Javni sastanak	Preko elektronske pošte	Datum održavanja 07.12.2018		
Pismena konsultacija sa javnošću na osnovu člana 7. i 32. i Poslovnika o radu Vlade Kosova br. 09/2011	Operateri esencijalnih usluga, provajderi digitalnih usluga, univerziteti, stručnjaci oblasti, široka javnost	Objavljivanje nacrta Koncept dokumenta u online platformi	Platforma online za javne konsultacije http://konsultimet.rks gov.net/viewConsult.php?ConsultationID=40535	30.11.2018 - 20.12.2018 (15. radnih dana)		

Poglavlje 6 : Upoređivanje opcija

Nedostatak koordinacije između sektora koji koriste infrastrukturu mreža i informacionih sistema kao kritičku infrastrukturu u preduzimanju mera za neprekidno podizanje i održavanje bezbednosti ove infrastrukture i nedovoljan pritisak odgovornim institucijama, uticali su na dosadašnje odlaganje zakonodavstva koje reguliše pitanja bezbednosti i zaštite mreža i IS.

Opcija da se nastavi ovo stanje povećava verovatnoću za neki kibernetički napad na mreže i sisteme PEU-a i PDU-a za nepredvidive posledice za e-ekonomiju.
Na osnovu analiza, procenjeno je da promena ovog stanja može se ostvariti kroz dve opcije:
1. Donošenja novog zakona, i
2. Promene postojećeg pristupa sprovođenju.

Održavanje aktuelne politike je promena samo postojećeg pristupa sprovođenja, neće dovesti nijedno poboljšanje stanja u pogledu povećanja nivoa bezbednosti mreža i informacionih sistema, a posebno onih koji se koriste kao kritična infrastruktura.
Zakon o kritičnoj infrastrukturi precizira opšte principe i kriterijume identifikacije kritične infrastrukture. Međutim, ovaj zakon ne dopunjuje zakon koji se očekuje da bude izrađen nakon usvajanja ovog KD-a, koji se fokusira samo na mere bezbednosti u mreži i informacionim sistemima koji se smatraju kritičnom infrastrukturom.
Uzimajući u obzir gore navedene probleme, opcija donošenja zakona, ostaje jedina opcija koju treba razmotriti.

Poglavlje 6.1: Plan sprovođenja preferirane opcije

Plan za sprovođenje jedine preferirane opcije (opcija 2) je prikazana u tabeli broj 8, u kojoj su precizirani ciljevi, proizvod, aktivnosti, vremenski rokovi kao i odgovorne institucije.

Slika 6: Plan sprovođenja za Opciju 2

Cilj politike	Promena postojećeg stanja u oblasti bezbednosti mreža i informacionih sistema							Iznos procenjenih troškova
Strateški cilj	Povećanje nivoa stabilnosti bezbednosti mreža i informacionih sistema							
	Proizvodi, aktivnosti, godina i odgovorna organizacija/odeljenje							
Strateški cilj 1 Poboljšanje bezbednosnih kapaciteta na nacionalnom nivou za oblast bezbednosti mreža i informacionih sistema koji su korišćeni kao kritična infrastruktura.	Proizvod 1.1 Odeljenje OPTIKT ovlašćeno dužnostima i odgovornostima nadzornog organa							
			Godina 1	Godina 2	Godina 3	Godina 4	Godina 5	Odgovorna institucija/ odeljenje	
		Aktivnost 1.1.1 Podizanje profesionalnih i tehničkih kapaciteta	x	x				MER	

		Aktivnost 1.1.2 Obuka i sertifikacija stručnog osoblja	x	x	x			MER	
		1.1.3. Dopunjavanje sekundarnog zakonodavstva	x	x	x			MER	
	Proizvod 1.2 KOS-Cert jedinica ovlašćena dužnostima i odgovornostima nacionalnog CSIRT-a								
			Viti 1	Viti 2	Viti 3	Viti 4	Viti 5	Odgovorna institucija/ odeljenje	
		Aktivnost 1.2.1 Podizanje profesionalnih i tehničkih kapaciteta		x	x			RAEPK	
		Aktivnost 1.2.2 Stručna obuka osoblja		x	x			RAEPK	
		Aktivnost 1.2.3. Sprovođenje bezbednosnih standarda za reagovanje	x	x	x	x	x	RAEPK	

		i izveštavanje o incidentima							
Strateški cilj 2 Unapređenje saradnje sa zemljama EU-a i drugim zemljama koje sprovode NIS direktivu	Proizvod 2.1 Jedina kontakt tačka u okviru OPTIKT-a	Aktivnost 2.1.1 Podizanje kapaciteta		x	x			MER	
		Aktivnost 2.1.2 Izgradnja radne infrastrukture		x	x			MER	
		Aktivnost 2.1.3 Informisanje i izveštavanje	x	x	x	x	x	MER	
	2.2 Mreža sektorskih CSIRT-ova	Aktivnost 2.2.2 Izveštavanje nacionalnom CSIRT-u			x	x	x	RAEPK	
Strateški cilj 3 Bezbednosne mere za upravljanje rizikom i obavezama PEU-a i PDU-a za izveštavanje o incidentima	Proizvod 3.1 Sprovođenje tehničkih i profesionalnih obaveza za uspostavljanje bezbednos	Aktivnost 3.1.1 Stalno povećanje nivoa bezbednosti koje KI poseduju.	x	x	x	x	x	MER & RAEPK	

	nih mera njihovih mreža.								
		Aktivnost 3.1.2 Izveštavanje o bezbednosnim merama i incidentima koji mogu napasti njihove KI.	x	x	x	x	x	MER & RAEPK	

Poglavlje 6.2: Tabela upoređivanja svih tri opcija

Opcija 1, Status Quo (bez promena) – u slučaju da se ne izradi nova politika za bezbednosne mere mreža i informacionih sistema, a posebno onih koje se koriste kao kritična infrastruktura, sasvim je sigurno da neće biti naglašenih promena ili unapređenje u povećanju nivoa bezbednosti esencijalnih usluga, koje se pružaju od PEU-a i PDU-a.

Opcija status quo ujedno predstavlja i stagnaciju u procesu evropskih integracija Kosova, gde je transponiranje NIS direktive neophodan korak ka napretku u integracionim procesima.

Opcija 2, Donošenje zakonskog akta o merama za bezbednost mreža i informacionih sistema – utvrdiće neophodni zakonski okvir o merama za bezbednost mreža i informacionih sistema koji se koriste kao kritična infrastruktura.
Transponiranje ove direktive predstavlja obavezu sa sve zemlje EU-a, uključujući i Kosovo, koje je preuzimalo obaveze, u cilju usklađivanja zakonodavstva sa EU zakonodavstvom.
NIS direktiva predstavlja temelje zaštite esencijalnih usluga i zlonamernih aktivnosti koje mogu doći kroz mreže, i reguliše interakcije sa državama koje sprovode ovu direktivu.
Transponiranje ove direktive u našem domaćem zakonodavstvu i njeno sprovođenje pružaće mogućnosti PEU-ima i PDU-ima da povećaju nivo bezbednosti usluga koje pružaju, kao i identifikaciju i sprečavanje zlonamernih aktivnosti, zaštitu i njihovo izveštavanje preko CSIRT mreže.

Opcija 3. Promena postojećeg pristupa sprovođenju – održavanje aktuelne politike i promena samo postojećeg pristupa sprovođenju, neće dovesti do nikakvog poboljšanja stanja u pogledu povećanja nivoa bezbednosti.

Slika 7:Upoređivanje opcija

Metoda upoređivanja:									
Relevantni pozitivni uticaji	Opcija 1: Bez promena			Opcija 2: Promena postojeće politike – donošenje zakonskog akta			Opcija 3: Promena postojećeg pristupa sprovođenju		
Povećanje nivoa bezbednosti MIS	ne			da			ne		
Identifikacija i izveštavanje o incidentima	ne			da			da		
Povećanje poverenja u pruženim uslugama	ne			da			ne		
Relevantni negativni uticaji									
Broj neidentifikovanih incidenata	da			ne			ne		
Relevantni troškovi	ne			da			da		
Procena očekivanog budžetskog uticaja	Godina 1	Godina 2	Godina 3	Godina 1	Godina 2	Godina 3	Godina 1	Godina 2	Godina 3
	ne	ne	ne	da	da	da	ne	ne	ne
Zaključak									

Poglavlje 7:Zaključci i naredni koraci

Poboljšanje postojećeg stanja kroz donošenje novog zakona uspostaviće neophodni zakonski okvir za povećanje bezbednosnih mera mreža i informacionih sistema koje se koriste kao Kritična infrastruktura.

Ovo bi upotpunilo postojeći zakonski okvir, koji bi poslužio kao osnova za podizanje kapaciteta, i ujedno će obavezivati PEU-ove i PDU-ove da povećaju bezbednosne mere njihovih mreža i informacionih sistema za pružanje usluga, kao i izveštavanje o mogućim incidentima.

Pored toga, ovaj zakon će regulisati i nivo saradnje sa CSIRT-ovima i njihovo izveštavanje na lokalnom i regionalnom nivou.

Plan sprovođenje preferirane opcije je plan sprovođenja Opcije 2, koja je prikazana na slici 8.

Poglavlje 7.1: Odredbe za praćenje i procenu

Prilog 1: Oblik procene za ekonomski uticaj

Kategorija ekonomskih uticaja	Glavni uticaj	Da li se ovaj efekat očekuje?		Broj ugroženih organizacija, kompanija i / ili pojedinaca	Očekivana beneficija ili troškovi uticaja	Preferirani nivo analize
		Da	Ne	visok/nizak	visok/nizak	
Radna mesta [1]	Da li će trenutni broj radnih mesta porastiti?	x		nizak	nizak	
	Da li će se sadašnji broj radnih mesta smanjiti?		x	/	/	
	Da li će uticati na nivo plaćanja?		x	/	/	
	Da li će uticati na olakšavanju pronalaska posla?	x		nizak	nizak	
Poslovanje	Da li će uticati na pristup u finansije za poslovanje?		x	/	/	
	Da li će neki određeni proizvodi biti izvučeni iz tržišta?		x	/	/	
	Da li će neki odredjeni proizvodi biti dozvoljeni na tržištu?	x		nizak	visok	
	Da li će preduzeća biti promorana da se zatvaraju?		x	/	/	

[1]Kada utiče na radna mesta, takođe će biti i društvenih uticaja.

	Hoće li se stvoriti nova preduzeća?		x	/	/	
Administrativno opterećenje	Da li će preduzeća biti primorana da ispune obaveze pružanja novih informacija?	x		nizak	visok	
	Da li su obaveze pružanja poslovnih informacija pojednostavljene?	x		nizak	visok	
Poslovanje	Da li se očekuje da trenutni tokovi uvoza promene?		x	/	/	
	Da li se očekuje da trenutni tokovi izvoza promene?		x	/	/	
Prevoz	Da li će uticati na način prevoza putnika i / ili robe?		x	/	/	
	Da li će biti nekih promena u vremenu potrebnom za prevoz putnika i / ili robe?		x	/	/	
Investicije	Da li se očekuje da kompanije ulažu u nove aktivnosti?	x		nizak	nizak	
	Da li se očekuje da kompanije otkažu ili odlože investicije za kasnije?		x	/	/	
	Da li će se povećati investicije iz dijaspore?		x	/	/	
	Da li će se smanjiti investicije iz dijaspore?		x	/	/	
	Da li će strane direktne investicije porastiti?	x		nizak	nizak	
	Da li će se strane direktne investicije smanjiti?		x	/	/	
Konkurentnost	Da li će se povećati poslovna cena proizvoda, kao što je električna energija?		x	/	/	

	Da li će se smanjiti cena poslovnih inputa, kao što je električna energija?		x	/	/	
	Da li postoje šanse da se promovišu inovacije i istraživanja?	x		nizak	visok	
	Da li postoje šanse da inovacija i istraživanja budu ometane?		x	/	/	
Uticaj na VMP	Da li su pogođena preduzeća uglavnom VMP		x	/	/	
Cene i konkurencija	Da li će broj roba i usluga koji su dostupni poslovanju ili korisnicima povećati?		x	/	/	
	Da li će se broj roba i usluga koji su dostupni poslovanju ili kupcima smanjiti?		x	/	/	
	Da li će se povećati cene roba i postojećih i usluga?	x		nizak	nizak	
	Da li će se smanjiti cene postojećih roba i usluga?		x	/	/	
Regionalni ekonomski uticaji	Da li će biti pod uticajem neki poseban sektor poslovanja?		x	/	/	
	Da li je ovaj sektor koncentrisan u određenom regionu?		x	/	/	
Opšti ekonomski razvoj	Da li će biti pod uticajem budući ekonomski rast?		x	/	/	
	Može li to imati bilo kakav efekat u stopi inflacije		x	/	/	

Prilog 2: Obrazac za procenu socijalnih uticaja

Kategorija društvenih uticaja	Glavni uticaj	Da li se ovaj efekat očekuje?		Broj ugroženih organizacija, kompanija i / ili pojedinaca	Očekivana beneficija ili troškovi uticaja	Preferirani nivo analize
		Da	Ne	visok/nizak	visok/nizak	
Radna mesta 2	Da li će trenutni broj radnih mesta porastiti?	x		nizak	nizak	
	Da li će trenutni broj radnih mesta smanjiti?		x	/	/	
	Da li su pod uticajem radna mesta u određenom poslovnom sektoru?		x	/	/	
	Da li će biti bilo kakav uticaj na nivo plaćanja?		x	/	/	
	Da li će uticati na olakšavanju pronalaska posla?		x	/	/	
Regionalni socijalni uticaji	Da li su socijalni uticaji usredsređeni na određenu regiju ili grad?		x	/	/	
Uslovi rada	Da li su radnička prava pogođena?		x	/	/	
	Da li su predviđeni ili ukinuti standardi za rad u opasnim uslovima?		x	/	/	
	Da li će imati uticaj na razvoj socijalnog dijaloga između zaposlenih i poslodavaca?		x	/	/	
Društvena uključenost	Da li će imati uticaj na siromaštvo?		x	/	/	
	Da li je pogođen pristup u programima socijalne zaštite?		x	/	/	
	Da li će se promeniti cena roba i osnovnih usluga?	x		nizak	nizak	
	Da li će imati uticaj na finansiranje ili organizaciju šema socijalne zaštite?		x	/	/	
Obrazovanje	Da li će imati uticaj na osnovno obrazovanje?		x	/	/	

[2]Kada utiče na radna mesta, takođe će uticati i u ekonomiju.

	Da li će imati uticaj na srednje obrazovanje?		x	/	/	
	Da li će imati uticaj na visoko obrazovanje?		x	/	/	
	Da li će imati uticaj na stručno usavršavanje?		x	/	/	
	Da li će imati uticaj na obrazovanje radnika i doživotno učenje?		x	/	/	
	Da li će imati uticaj na organizaciju ili strukturu obrazovnog sistema?		x	/	/	
	Da li će imati uticaj na akademsku slobodu i samoupravu?		x	/	/	
Kultura	Da li opcija utiče na kulturnu raznolikost?		x	/	/	
	Da li opcija utiče na mogućnost finansiranja kulturnih organizacija?		x	/	/	
	Da li opcija utiče na mogućnost da ljudi imaju beneficije od kulturnih aktivnosti ili učestvuju u njima?		x	/	/	
	Da li opcija utiče na mogućnost očuvanja kulturnog nasleđa?		x	/	/	
Vladavina	Da li opcija utiče u sposobnosti građana da učestvuju u demokratskom procesu?		x	/	/	
	Da li se svaka osoba jednako tretira?		x	/	/	
	Da li će se javnost bolje informisati o određenim pitanjima?		x	/	/	
	Da li opcija utiče na način kako funkcionisaju političke stranke?		x	/	/	

	Da li će imati uticaj na civilno društvo?		x	/	/	
Zdravlje i javna bezbednost 3	Da li će imati uticaj na u ljudskim životima, kao što je životni vek ili stopa smrtnosti?		x	/		
	Da li će imati uticaj na kvalitet hrane?		x	/	/	
	Da li će se rizik od zdravstvenog stanja povećati ili smanjiti zbog štetnih supstanci?		x	/	/	
	Da li će uticati na zdravlje zbog promena nivoa buke ili kvaliteta vazduha, vode i / ili zemlje?		x	/	/	
	Da li će biti zdravstvenih efekata zbog promene u upotrebi energije?		x	/	/	
	Da li će doći do zdravstvenih efekata zbog promena u deponisanju otpada?		x	/	/	
	Da li će imati uticaj na način života ljudi, kao što su nivoi interesa u sportu, promene u ishrani ili promene u upotrebi duvana ili alkohola?		x	/	/	
	Postoje li određene grupe koje se suočavaju sa većim rizicima od drugih (određeni faktorima kao što su godina, pol, invaliditet, društvena grupa ili region)?		x	/	/	
Kriminal i bezbednost	Da li se pogađaju šanse za hvatanje kriminalca?		x	/	/	

[3]Kada utiče na javno zdravlje i bezbednost, on redovno ima uticaj na životnu sredinu.

	Da li ima uticaj potencijalni profit iz kriminala?		x	/	/	
	Da li utiče na nivo korupcije?		x			
	Da li ima uticaj sposobnost sprovođenja zakona?		x	/	/	
	Ima li uticaj na prava i sigurnost žrtava kriminaliteta?		x	/	/	

Prilog 3: Obrazac za procenu uticaja na životnu sredinu

Kategorija uticaja na životnu sredinu	Glavni uticaj	Da li se ovaj efekat očekuje?		Broj ugroženih organizacija, kompanija i / ili pojedinaca	Očekivana korist ili troškovi uticaja	Preferirani nivo analize
		Da	Ne	visok/nizak	visok/nizak	
Klima i održivo okruženje	Da li će uticati na emisije gasova staklene bašte (ugljen-dioksid, metan itd.)?		x	/	/	
	Da li će uticati na potrošnju goriva?		x	/	/	
	Da li će se promeniti raznolikost resursa koji se koriste za proizvodnju energije?		x	/	/	
	Da li će doći do promena cena za prijateljske proizvode za životnu sredinu?		x	/	/	
	Da li će određene aktivnosti biti manje zagađivane?		x	/	/	
Kvalitet vazduha	Da li će imati uticaj na emisiju zagađivača vazduha?		x	/	/	
Kvalitet vode	Da li opcija utiče na kvalitet slatke vode?		x	/	/	
	Da li opcija utiče na mogućnost kvaliteta podzemnih voda?		x	/	/	

	Da li opcija utiče na resurse pitke vode?		x	/	/	
Kvalitet zemljišta i korišćenje zemljišta	Da li će to uticati na kvalitet zemljišta (u smislu zakisljenja, kontaminacije, upotrebe pesticida ili herbicida)?		x	/	/	
	Da li će imati uticaj na eroziju zemljišta?		x	/	/	
	Hoće li izgubiti zemlju (kroz izgradnju itd.)?		x	/	/	
	Da li se zemljište može dobiti (kroz dekontaminaciju itd.)?		x	/	/	
	Da li će doći do promene u korištenju zemljišta (npr. Od šumskog korištenja šuma u poljoprivredno ili urbane korištenje)?		x	/	/	
Otpad i reciklaža	Da li će se promeniti količina nastalog otpada?		x	/	/	
	Da li će se promeniti načini na koji se rukovoditi otpad?		x	/	/	
	Da li će imati uticaj na mogućnosti za reciklažu otpada?		x	/	/	
Korišćenje resursa	Da li opcija utiče u korištenje obnovljivih izvora (riblje rezerve, hidroelektrane, solarna energija itd.)?		x	/	/	
	Da li opcija utiče u korištenje neobnovljivih izvora (podzemnih voda, minerala, uglja itd.)?		x	/	/	
Stepen sredinskih rizika	Da li ima bilo kakav uticaj na verovatnoću opasnosti, kao što su požari, eksplozije ili nesreća?		x	/	/	

	Da li će uticati na spremnost u slučaju prirodnih nepogoda?		x	/	/	
	Da li ima uticaja zaštita društva od prirodnih nepogoda?		x	/	/	
Bioraznolikost, flora i fauna	Da li će imati uticaj na zaštićene ili ugrožene vrste ili na područja u kojima žive?		x	/	/	
	Da li će biti dirnuta veličina ili veze između prirodnih područja?		x	/	/	
	Da li će imati neki uticaj na broj vrsta u određenom području?		x	/	/	
Dobrobit životinja	Da li će uticati postupanje sa životinjama?		x	/	/	
	Da li će uticati na zdravlje životinja?		x	/	/	
	Da li će uticati na kvalitet i sigurnost životinjske hrane ?		x	/	/	

Prilog 4: Obrazac procene za uticaj osnovnih prava

Kategorija uticaja na osnovna prava	Glavni uticaj	Da li se ovaj efekat očekuje?		Broj ugroženih organizacija, kompanija i / ili pojedinaca	Očekivana korist ili troškovi uticaja	Preferirani nivo analize
		Da	Ne	visok/nizak	visok/nizak	
Dostojanstvo	Da li opcija utiče na dostojanstvo ljudi, na njihovo pravo na život ili integritet lica?		x	/	/	
Sloboda	Da li opcija utiče na pravo na slobodu pojedinaca?		x	/	/	
	Da li opcija utiče na prava lica za privatnost	x		visok	visok	
	Da li opcija utiče na pravo na sklapanje braka ili imati porodicu?		x	/	/	

	Da li opcija utiče na pravnu, ekonomsku ili socijalnu zaštitu pojedinaca ili porodice?		x	/	/	
	Da li opcija utiče na slobodu misli, savesti ili veroispovesti?		x	/	/	
	Da li opcija utiče na slobodu izražavanja?		x	/	/	
	Da li opcija utiče na slobodu okupljanja ili udruživanja?		x	/	/	
Lični podaci	Da li opcija obuhvata obradu ličnih podataka?	x		nizak	visok	
	Da li su zagarantovana prava pojedinca na pristup, ispravku i prigovoru?	x		nizak	visok	
	Da li je jasan i zaštićen način na kojima se obrađuju lični podaci?	x		visok	visok	
Azil	Da li ova opcija utiče na pravo na azil?		x	/	/	
Imovinska prava	da li ce imati uticaj u imovinska prava		x	/	/	
	Da li opcija utiče na slobodu poslovanja?		x	/	/	
Jednak tretman [4]	Da li opcija štiti princip jednakosti pred zakonom?	x		visok	visok	
	Jel ima šanse da određene grupe mogu biti direktno ili indirektno pogođene diskriminacijom (npr. Rod, rasa, boja, etnička pripadnost, političko ili drugo mišljenje, doba života, seksualna orijentacija)?		x	/	/	
	Da li opcija utiče na prava lica sa invaliditetom?		x	/	/	
Dečija prava	Da li opcija utiče na dečija prava?		x	/	/	

[4]Rodna ravnopravnost se tretira u proceni polnog uticaja

Dobra uprava	Da li će administrativni postupci postati komplikovaniji?		x	/	/	
	Da li će biti po uticajem nacin na koji administracija donosi odluke (transparentnost, proceduralni rok, pravo na pristup dosijima itd.)?		x	/	/	
	Za krivično pravo i predviđene kazne: da li su pod uticajem prava optuženog?		x	/	/	
	Da li je ugrožen pristup u pravdu?		x	/	/	