BOSNA I HERCEGOVINA

REVIZIJA UČINKA

AKTIVNOSTI INSTITUCIJA BIH NA OSIGURANJU OSNOVNIH PRETPOSTAVKI ZA KIBERSIGURNOST

URED ZA REVIZIJU INSTITUCIJA BIH
КАНЦЕЛАРИЈА ЗА РЕВИЗИЈУ ИНСТИТУЦИЈА БИХ
AUDIT OFFICE OF THE INSTITUTIONS OF BOSNIA AND HERZEGOVINA

www.revizija.gov.ba

Naslovnica: rawpixel.com on Freepik

URED ZA REVIZIJU INSTITUCIJA BIH
КАНЦЕЛАРИЈА ЗА РЕВИЗИЈУ ИНСТИТУЦИЈА БИХ
AUDIT OFFICE OF THE INSTITUTIONS OF BOSNIA AND HERZEGOVINA

www.revizija.gov.ba

IZVJEŠTAJ REVIZIJE UČINKA

„AKTIVNOSTI INSTITUCIJA BOSNE I HERCEGOVINE NA OSIGURANJU OSNOVNIH PRETPOSTAVKI ZA KIBERSIGURNOST“

Broj: 05-16-1-1431/22

Sarajevo, decembar 2022. godine

Aktivnosti institucija BiH na osiguranju osnovnih pretpostavki za kibersigurnost

Ured za reviziju institucija BiH je proveo reviziju učinka na temu: „Aktivnosti institucija BiH na osiguranju osnovnih pretpostavki za kibersigurnost“. Revizija je provedena u skladu sa Zakonom o reviziji institucija BiH, Međunarodnim standardima vrhovnih revizionih institucija – ISSAI, INTOSAI smjernicama i metodologiji za rad revizije učinka vrhovnih revizionih institucija u BiH.

Ured za reviziju institucija BiH je proveo reviziju s ciljem provjere jesu li institucije BiH efikasne u preduzimanju aktivnosti s ciljem osiguranja osnovnih pretpostavki za kibersigurnost.

Nalazi revizije ukazuju na to da institucije BiH nisu bile efikasne u preduzimanju aktivnosti s ciljem osiguranja osnovnih pretpostavki za kibersigurnost. Nedostaje strateški i zakonski okvir kibersigurnosti, a nije uspostavljen ni Tim za računarske incidente za institucije BiH. Institucije BiH su imale pasivan pristup u donošenju akata upravljanja informacionom sigurnošću u skladu s Politikom upravljanja informacionom sigurnošću i/ili standardima upravljanja informacionom sigurnošću. Samo 14 od 68 institucija BiH je donijelo akte upravljanja informacionom sigurnošću u skladu s Politikom upravljanja informacionom sigurnošću.

Posljedice nedostatka osnovnih pretpostavki za kibersigurnost ugrožavaju poslovanje javne uprave i mogu dovesti do otuđenja podataka i finansijskih sredstava neophodnih za funkcionisanje zemlje i svakodnevnog života građana.

Izvještaj revizije sadrži preporuke upućene Vijeću ministara BiH, Ministarstvu komunikacija i prometa BiH, Ministarstvu sigurnosti BiH i institucijama BiH. Realizacijom preporuka trebalo bi se pridonijeti osiguranju osnovnih pretpostavki za kibersigurnost i unapređenju kiberzaštite u institucijama BiH. Implementacija preporuka trebala bi doprinijeti i realizaciji Ciljeva održivog razvoja, a naročito ciljevima održivog investiranja u infrastrukturu i inovacije i razvoju učinkovitih, odgovornih i transparentnih institucija i omogućavanju pristupa informacijama.

Ured za reviziju je, u skladu s odredbama Zakona o reviziji institucija BiH, dostavio Nacrt izvještaja institucijama koje su bile obuhvaćene provedenom revizijom. Ovim institucijama je ostavljena mogućnost da daju svoje komentare i primjedbe na nalaze i zaključke obavljene revizije. Nakon toga je izrađen konačan izvještaj o provedenoj reviziji učinka.

GENERALNI REVIZOR

Hrvoje Tvrtković, v.r.

ZAMJENIK GENERALNOG REVIZORA

Jasmin Pilica, v.r.

ZAMJENIK GENERALNOG REVIZORA

Ranko Krsman, v.r.

Sadržaj

Korištene skraćenice

Skraćenica	Puni naziv
AJN	Agencija za javne nabavke Bosne i Hercegovine
AZLP	Agencija za zaštitu ličnih podataka u Bosni i Hercegovini
BiH	Bosna i Hercegovina
CERT	Tim za odgovor na računarske incidente
Direktiva NIS	Direktiva o mjerama za visok zajednički nivo sigurnosti mrežnih i informacionih sistema širom Unije
EK	Evropska komisija
EU	Evropska unija
GS	Generalni sekretarijat Vijeća ministara Bosne i Hercegovine
ISO	Međunarodna organizacija za standardizaciju (International Organization for Standardization)
IT	Informacione tehnologije
MFT	Ministarstvo finansija i trezora Bosne i Hercegovine
MKP	Ministarstvo komunikacija i prometa Bosne i Hercegovine
MS	Ministarstvo sigurnosti Bosne i Hercegovine
OSCE	Organizacija za sigurnost i saradnju u Evropi
Politika upravljanja informacionom sigurnošću	Politika upravljanja informacionom sigurnošću u institucijama BiH za period 2017 – 2022. godina
RAK	Regulatorna agencija za komunikacije Bosne i Hercegovine
RH	Republika Hrvatska
Sjevernoatlantski savez	NATO
Služba za e-vladu pri GS	Služba za održavanje i razvoj elektronskog poslovanja i e-vlade pri Generalnom sekretarijatu Vijeća ministara Bosne i Hercegovine
Sl. gl. BiH	Službeni glasnik Bosne i Hercegovine
UNDP	Program Ujedinjenih naroda za razvoj
VM	Vijeće ministara Bosne i Hercegovine

Izvršni rezime

Ured za reviziju institucija BiH je proveo reviziju učinka s ciljem da utvrdi jesu li institucije BiH efikasne u preduzimanju aktivnosti s ciljem osiguranja osnovnih pretpostavki za kibersigurnost.

U nastavku su najvažniji nalazi i preporuke revizije:

- Aktivnosti na donošenju strateškog i zakonskog okvira kibersigurnosti pokrenute su još 2017. godine, a pet godina nakon toga aktivnosti nisu okončane i strateški i zakonski okvir kibersigurnosti još uvijek nije donesen.
- Ni nakon pet godina od zaduženja VM-a odgovorne institucije BiH nisu izradile strateški i zakonski okvir kibersigurnosti i izvjesno je da dinamika aktivnosti odgovornih institucija BiH neće osigurati završetak ovih aktivnosti u trenutno definisanom roku.
- Na nivou institucija BiH ni nakon pet godina od donošenja Odluke VM-a o određivanju CERT-a za institucije BiH nije uspostavljen CERT koji bi učinkovito koordinirao i upravljao pružanjem odgovora na računarske incidente.
- Iako je VM zadužio MS da u kratkom roku preduzme aktivnosti s ciljem uspostave CERT-a za institucije BiH, MS za pet godina nije osigurao potrebne uslove za uspostavu CERT-a.
- Institucije BiH su imale pasivan pristup u donošenju akata upravljanja informacionom sigurnošću u skladu s Politikom upravljanja informacionom sigurnošću i/ili standardima upravljanja informacionom sigurnošću.
- Samo 14 od 68 institucija BiH je donijelo akte upravljanja informacionom sigurnošću u skladu s Politikom upravljanja informacionom sigurnošću.

Ured za reviziju institucija BiH je definisao preporuke s ciljem da se pridonese osiguranju osnovnih pretpostavki za kibersigurnost i unapređenju kiberzaštite u institucijama BiH. Preporuke su upućene Vijeću ministara BiH, Ministarstvu komunikacija i prometa BiH, Ministarstvu sigurnosti BiH i institucijama BiH.

Preporuka Vijeću ministara BiH

- Definisati rokove za pripremu i odgovornost za izvještavanje o procesu pripreme relevantnih akata kibersigurnosti.

Preporuke Ministarstvu komunikacija i prometa BiH i Ministarstvu sigurnosti BiH

- Žurno okončati pripremu prijedloga relevantnih propisa kibersigurnosti i dostaviti ih Vijeću ministara na usvajanje.
- Izvijestiti VM o realizaciji Politike upravljanja informacionom sigurnošću u institucijama BiH.

Preporuke Ministarstvu sigurnosti BiH

- Žurno okončati pripremu prijedloga strateškog okvira kibersigurnosti i dostaviti ga Vijeću ministara na usvajanje.
- Žurno osigurati organizacione pretpostavke za formiranje Tima za odgovor na računarske incidente za institucije BiH.

Preporuka institucijama BiH

- Žurno donijeti akte upravljanja informacionom sigurnošću u skladu s Politikom upravljanja informacionom sigurnošću.

1. UVOD

1.1. Pozadina problema i motivi za studiju

Svakodnevna upotreba informacionih tehnologija otvara čitav niz novih mogućnosti, ali i prijetnji od kibernapada i kiberkriminala od kojih posljedice mogu imati zastrašujuće implikacije na društvo i gospodarstvo.[1] Kibersigurnost predstavlja vrlo važnu komponentu u korištenju informacionih tehnologija i zaštiti podataka od mogućih krađa, povrede informacione sigurnosti i raznih malverzacija koje imaju negativan društveni, gospodarski i politički učinak. Značaj kibersigurnosti je posebno došao do izražaja u vrijeme epidemije koronavirusa zbog povećane ovisnosti o informacionoj tehnologiji.

Bosna i Hercegovina (BiH) značajno zaostaje za ostalim zemljama Evrope u digitalnoj transformaciji društva pa tako i u kibersigurnosti.[2] Povećan broj kiberprijetnji i nedostaci u kiberzaštiti u BiH su teme u fokusu medija.[3] U BiH ne postoje službeni podaci o broju i vrsti kibernapada. Neslužbeni podaci govore da se broj kibernapada u BiH povećao za 1300 puta na sedmičnoj osnovi. Od 68 institucija BiH, 24 institucije BiH su imale zabilježene kibernapade.[4] Koliko je ovaj problem aktualan govori u prilog činjenica da su u toku pripreme ovog izvještaja zabilježeni kibernapadi na institucije BiH.[5] Posljednji zabilježeni kibernapad na institucije BiH obustavio je rad zaposlenih, a onemogućio pristup službenim stranicama skoro mjesec dana.[6]

Javna uprava je jedan od ključnih čimbenika za razvoj informacionog društva i kao takva snosi odgovornost za kibersigurnost. BiH se u skladu sa svojim opredjeljenjem za pristupanje Evropskoj uniji (EU) obavezala na unapređenje kibersigurnosti. U BiH, bez obzira na opredjeljenje za pristupanje EU, još uvijek nisu osigurane osnovne pretpostavke za kibersigurnost,[7] iako je centralni pravni akt o kibersigurnosti EU donesen još 2016.

---

[1] Procjena je da će finansijski učinak kiberkriminala na svjetsko gospodarstvo dosegnuti šest biliona američkih dolara godišnje do 2021, podaci dostupni na linku: The 2020 Official Annual Cybercrime Report - Herjavec Group

[2] BiH se nalazi na devetom mjestu u svijetu po riziku od kiberprijetnji ili na 86. mjestu po kibersigurnosti i značajno zaostaje za zemljama iz okruženja, dostupno na linku: https://cybernews.com/news/should-you-worry-100-countries-ranked-by-cyber-safety/

[3] BiH jedina država bez strategije o zaštiti računarskih podataka - Pogled.ba
Cyber napadi su realna i postojeća prijetnja za BiH | TEME | Al Jazeera
https://atlantskainicijativa.org/cyber-napadi-kao-rastuca-teroristicka-prijetnja-nespremnim-balkanskim-zemljama/
https://balkans.aljazeera.net/news/technology/2021/10/29/bosna-i-hercegovina-medju-najmanje-sigurnim-od-cyber-kriminala
Ugroženi privatni podaci 15.000 osoba iz BiH: Hakerski napad na servere Crvenog krsta | DEPO Portal
https://www.klix.ba/vijesti/bih/arnautovic-dobili-smo-informaciju-o-cyber-napadima-na-centralnu-izbornu-komisiju/220527130

[4] Prema podacima iz Upitnika revizije učinka na temu kibersigurnost, od 73 institucije BiH kojim je poslan Upitnik, 68 institucija je dostavilo odgovore na Upitnik.

[5] Izveden hakerski napad na servere Parlamenta BiH - www.vecernji.ba
SIPA odbila hakerski napad na ovu policijsku agenciju! (avaz.ba)

[6] https://inforadar.ba/institucije-bih-u-blokadi-vec-17-dana-server-cik-a-moguci-glavi-cilj-hakerskog-napada/
https://bljesak.info/vijesti/flash/zaposlenici-u-drzavnim-institucijama-vec-dva-tjedna-ne-rade-nista-zbog-hakerskog-napada/394589

[7] U Izvještaju o napretku BiH za 2021. godinu navedeno je da nije postignut napredak u oblasti kibersigurnosti. Izvještaj dostupan na linku: izvjestaj-o-bosni-i-hercegovini-za-2021-godinu_1636467943.pdf (dei.gov.ba)

godine.[8] Donošenjem odluka i zaključaka iz oblasti kibersigurnosti 2017. godine, Vijeće ministara BiH (VM) se opredijelilo za jačanje kibersigurnosti institucija BiH, ali još uvijek nije donesen strateški, zakonski i organizacioni okvir kibersigurnosti.[9]

Institucije BiH za poslovanje koriste informacione sisteme čija sigurnost je od izuzetnog značaja. Ugrožavanjem sigurnosti informacionih sistema institucija BiH nastupile bi ozbiljne posljedice za funkcionisanje javne uprave i gospodarstva. Naprimjer, ugrožavanje sigurnosti sistema e-vlada uzrokovalo bi zastoj u radu VM-a i moglo bi se kasniti u donošenju važnih odluka za javnu upravu i građane. Napad na informacioni sistem Ministarstva finansija i trezora BiH (MFT) ugrozio bi evidencije svih finansijskih transakcija institucija BiH i mogao bi uzrokovati obustavu svih plaćanja iz budžeta BiH.

Rezultati predstudijskih istraživanja Ureda za reviziju institucija BiH također su ukazali na probleme u uspostavi kibersigurnosti institucija BiH.

Imajući na umu sve navedeno, Ured za reviziju institucija BiH donio je Odluku o provođenju revizije učinka u oblasti kibersigurnosti institucija BiH.

1.2. Cilj, obim i ograničenja revizije

1.2.1. Cilj revizije

Cilj revizije je pokazati jesu li institucije BiH efikasne u preduzimanju aktivnosti s ciljem osiguranja osnovnih pretpostavki za kibersigurnost.

Svrha revizije je doprinijeti stvaranju kiberzaštite i jačanju kiberotpornosti institucija BiH kako bi se zaštitile institucije BiH, građani i ugled države.

Provođenje ove revizije trebalo bi doprinijeti realizaciji ciljeva održivog razvoja, a naročito ciljevima održivog investiranja u infrastrukturu i inovacije (cilj 9) i razvoju učinkovitih, odgovornih i transparentnih institucija i omogućavanju pristupa informacijama (cilj 16).

1.2.2. Obim i ograničenja revizije

Predmet revizije su aktivnosti institucija BiH na osiguravanju osnovnih pretpostavki za kibersigurnost. U kontekstu ove studije osnovne pretpostavke se odnose na osiguravanje strateškog i zakonskog okvira kibersigurnosti, Tima za odgovor na računarske incidente (CERT) i sistema upravljanja informacionom sigurnošću u institucijama BiH. S obzirom na to da je oblast kibersigurnosti široko područje revizija se nije bavila drugim mogućim pretpostavkama za kibersigurnost.

Analizirale su se aktivnosti odgovornih institucija BiH iz oblasti kibersigurnosti u osiguranju osnovnih pretpostavki za kibersigurnost. Promatrale su se aktivnosti VM-a koji je odgovoran za donošenje strateških odluka i zakonskih propisa u oblasti kibersigurnosti, određivanje rokova i odgovornosti za izvještavanje. Predmet analiza bile su i aktivnosti institucija BiH na uspostavi preventivnih mjera kibersigurnosti i donošenju akata

[8] Direktiva o mjerama za visok zajednički nivo sigurnosti mrežnih i informacionih sistema širom Unije je prvi zakon o kibersigurnosti na nivou EU i predstavlja glavni stub Strategije za kibersigurnost EU iz 2013. godine.
[9] Odluka o određivanju Tima za odgovor na računarske incidente za institucije BiH, Odluka o usvajanju Politike upravljanja informacionom sigurnošću u institucijama BiH za period 2017 – 2022. godine i Zaključak VM-a da se intenziviraju aktivnosti na izradi Strategije kibersigurnosti.

upravljanja informacionom sigurnošću. Analizirale su se informacije iz upitnika, kojim su ispitane 73 institucije BiH[10], a koje su relevantne za uspostavu kibersigurnosti.

Detaljnije su se analizirale aktivnosti institucija iz uzorka na uspostavi preventivnih mjera kibersigurnosti i donošenju akata upravljanja informacionom sigurnošću. Implementacija preventivnih mjera kibersigurnosti koje su preduzete u institucijama iz uzorka nije bila predmetom detaljnije analize.

U uzorak su izabrane institucije prema više kriterija. Ministarstvo komunikacija i prometa BiH (MKP) i Ministarstvo sigurnosti BiH (MS) su odgovorne institucije BiH u oblasti kibersigurnosti. Agencija za javne nabavke BiH (AJN) je institucija visokog sigurnosnog rizika jer su informacioni sistemi otvoreni za sve učesnike javnih nabavki u BiH. Agencija za zaštitu ličnih podataka BiH (AZLP) je institucija koja posjeduje registre ličnih podataka zbog čega je izuzetno važna kiberzaštita i primjer dobre prakse. Ministarstvo finansija i trezora BiH (MFT) je institucija u kojoj je zabilježen kibernapad[11]. MFT također upravlja informacionim sistemima za plaćanja iz budžeta institucija BiH u milionskim iznosima. Generalni sekretarijat VM-a BiH (GS) upravlja sistemom e-vlade čije servise koristi oko 58 institucija BiH. GS, između ostalog, utvrđuje način zaštite sistema e-vlade i pravila korištenja servisa e-vlade za korisnike. Regulatorna agencija za komunikacije BiH (RAK) je institucija koja po poslovima koje obavlja spada u kritičnu infrastrukturu i institucija koja je nedavno donijela okvir upravljanja informacionom sigurnošću.

Revizija se nije bavila aktivnostima institucija BiH u oblasti kiberkriminala. Revizija nije analizirala regulativu koja se dodiruje sa kibersigurnošću, kao što je regulativa koja se odnosi na elektronsko poslovanje, komunikacije i zaštitu ličnih podataka. Nisu analizirane aktivnosti institucija BiH u uspostavi kibersigurnosti podataka koji su zaštićeni oznakom tajnosti.

Nije bilo ograničenja revizije.

1.3. Reviziona pitanja i kriteriji revizije

Revizija će dati odgovor na jedno glavno pitanje i tri reviziona potpitanja. Glavno reviziono pitanje je:

Jesu li institucije BiH efikasne u preduzimanju aktivnosti s ciljem osiguranja osnovnih pretpostavki za kibersigurnost?

Za što bolje razumijevanje i analizu problema, te da bi se olakšalo prikupljanje potrebnih podataka, definisana su tri reviziona potpitanja:

1. Je li donesen strateški i zakonski okvir kibersigurnosti institucija BiH?
2. Je li uspostavljen Tim za odgovor na računarske incidente za institucije BiH?
3. Jesu li doneseni akti upravljanja informacionom sigurnošću u institucijama BiH?

[10] Od 73 ispitane institucije svoje odgovore je dostavilo 68 institucija. Odgovore nisu dostavile Agencija za antidoping kontrolu BiH, Agencija za prevenciju korupcije i koordinaciju borbe protiv korupcije BiH, Centar za uklanjanje mina u BiH, Institut za nestale osobe BiH i Služba za zajedničke poslove institucija BiH. Upitnikom nisu ispitane Obavještajno-sigurnosna agencija i Ured za reviziju institucija BiH.

[11] Izvršeno nekoliko napada na e-mail i web-stranicu MFT-a.

Kriteriji

Kriteriji revizije koje smo koristili u procjeni predmeta revizije zasnovani su na Direktivi o mjerama za visok zajednički nivo sigurnosti mrežnih i informacionih sistema širom Unije (NIS direktiva), preporukama Evropske komisije (EK) u oblasti kibersigurnosti, Odluci VM-a o određivanju CERT-a za institucije BiH iz 2017. godine, Odluci VM-a o usvajanju Politike upravljanja informacionom sigurnošću iz 2017. godine, Zaključku VM-a iz 2017. godine kojim se intenziviraju aktivnosti na izradi strateškog okvira kibersigurnosti, Smjernicama za strateški okvir kibersigurnosti u BiH, Izvještaju o ocjeni spremnosti za uspostavljanje CERT mreže u BiH, Pregledu kapaciteta kibersigurnosti u BiH i razgovorima s predstavnicima institucija iz uzorka i akademskoj literaturi o kibersigurnosti i informacionoj sigurnosti.[12]

Pod efikasnim preduzimanjem aktivnosti u kontekstu ove studije se podrazumijeva blagovremen[13] i proaktivan[14] odnos institucija BiH u preduzimanju aktivnosti potrebnih za osiguranje osnovnih pretpostavki za kibersigurnost.

Kriterij za prvo reviziono potpitanje:[15]

Donesen je strateški okvir kojim se osigurava sistemski pristup u izgradnji kibersigurnosti i podiže svijest o važnosti kibersigurnosti u institucijama BiH u skladu sa definisanim rokovima. Donesen je zakonski okvir kojim se osigurava provođenje mjera za postizanje visokog zajedničkog nivoa mrežne i informacione sigurnosti i nadležni organi za provođenje i nadzor mjera mrežne i informacione sigurnosti u institucijama BiH u skladu sa definisanim rokovima.

[12] Arbanas K. "Radni okvir za procjenu i unapređenje kulture informacijske sigurnosti" Disertacija, Sveučilište u Zagrebu, Fakultet organizacije i informatike, 2021. godine

[13] U skladu sa definisanim rokovima VM-a na koja se referiramo u izvorima kriterija za reviziona pitanja.

[14] U konstantnom toku aktivnosti i inicijative na rješavanju problema.

[15] VM je u 2017. godini donio zaključak kojim se zadužuje MS da intenzivira aktivnosti na izradi Strategije kibersigurnosti. Odlukom VM-a o usvajanju Politike upravljanja informacionom sigurnošću iz 2017. godine zadužuju se MKP i MS da izrade zakon o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema. U Programu rada MKP-a za 2018. godinu jedna od aktivnosti je bila izrada Nacrta zakona o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema. VM je u 2019. godini nakon razmatranja Informacije o ispunjavanju pravnog kriterija institucija BiH u procesu pridruživanja EU zadužio MKP da do kraja 2019. godine dostavi VM-u na usvajanje Nacrt zakona o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema. Prema preporukama EK-a u oblasti kibersigurnosti BiH treba usvojiti strategiju kibersigurnosti, izraditi akcione planove na svim nivoima vlasti i usvojiti zakon o kibersigurnosti. Usvajanjem preporuka EK-a iz 2019. godine, VM je usvojio i listu aktivnosti prema kojoj je prvobitni rok za realizaciju preporuka 2020. godina, a zatim 2021 / 2022. godina. Odgovorne institucije su MS i MKP. U Programu rada MS-a za 2021. godinu jedna od aktivnosti je bila izrada nacrta zakona o mrežnoj i informacionoj sigurnosti u institucijama BiH.

Kriterij za drugo reviziono potpitanje:[16]

Na nivou institucija BiH je uspostavljen operativan CERT za institucije BiH koji provodi aktivnosti upravljanja i koordiniranja prevencije i zaštite od sigurnosnih rizika u informacionim komunikacionim sistemima institucija BiH i ostale značajne aktivnosti u osiguranju kibersigurnosti. Uspostavljena je mreža CERT-ova u BiH koja vrši razmjenu informacija o incidentima i doprinosi razvoju pouzdanja i povjerenja među učesnicima mreže u BiH, i ostvaruje saradnju sa EU CERT-om i Agencijom EU za mrežnu i informacionu sigurnost. Navedeni organi su uspostavljeni u skladu sa definisanim rokovima.

Kriterij za treće reviziono potpitanje:[17]

Institucije BiH su proaktivno donosile akte upravljanja informacionom sigurnošću u skladu s Politikom upravljanja informacionom sigurnošću. Institucije BiH su izradile akte na osnovu smjernica i/ili međunarodnih standarda informacione sigurnosti s ciljem uspostave sistema upravljanja informacionom sigurnošću. MKP i MS su pratili implementaciju Politike upravljanja informacionom sigurnošću u institucijama BiH i o realizaciji redovno izvještavali VM.

1.4. Izvori informacija i metode revizije

Primarne metode revizije, koje je koristio revizioni tim u cilju osiguranja informacija za dobijanje odgovora na postavljena reviziona pitanja, su intervjui sa predstavnicima institucija BiH, ispitivanje kroz upitnik i dokumentarni pregledi.

Podaci dobijeni iz intervjua s predstavnicima institucija mjerodavnim za oblast kibersigurnosti i institucija iz uzorka su upoređeni s podacima iz prikupljene dokumentacije iz institucija iz uzorka, upitnika i drugih izvora. Podaci i informacije dobijeni iz dokumentarnog pregleda i intervjua s predstavnicima institucija iz uzorka su međusobno upoređivani.

Podaci su prikupljani pregledom i analizom sadržaja dokumentacije institucija mjerodavnih u oblasti kibersigurnosti i institucija iz uzorka, pregledom i analizom

[16] Odlukom VM-a o određivanju CERT-a za institucije BiH iz 2017. godine MS je trebao u roku od tri mjeseca dostaviti VM-u na usvajanje prijedlog dopuna Pravilnika o unutrašnjoj organizaciji MS-a s ciljem uspostave CERT-a. Programom rada MS-a za 2017. godinu bila je planirana aktivnost izrade odluka i akata unutrašnje organizacije s ciljem uspostave CERT-a. Aktivnosti na izradi odluke o uspostavljanju mreže CERT-ova je planirana u Programu rada MS-a za 2021. godinu. Prema preporukama EK-a u oblasti kibersigurnosti BiH treba uspostaviti CERT-ove, odrediti državne nadležne organe i pojedinačne kontakt tačke. Usvajanjem preporuka EK-a iz 2019. godine, VM je usvojio i listu aktivnosti prema kojoj je prvobitni rok za realizaciju preporuka 2020. godina, zatim 2021. godina, a odgovorna institucija je MS. Akcionim planom reforme javne uprave 2018 – 2022. planirana je aktivnost uspostave CERT-a do kraja 2022. godine.

[17] Prema Politici upravljanja informacionom sigurnošću iz 2017. godine preporučuje se institucijama BiH da implementiraju politike upravljanja informacionom sigurnošću na unaprijed izrađenim standardima u cilju uspostave sistema upravljanja informacionom sigurnošću u skladu s uočenim zahtjevima i potrebama svake institucije pojedinačno. Politikom upravljanja informacionom sigurnošću su ponuđene osnovne smjernice za izradu akata na osnovu međunarodnih priznatih standarda. MKP i MS su zaduženi za detaljnu izradu smjernica. MKP je predvodio aktivnosti i odlučilo se izraditi 11 smjernica u tri seta. Programom rada MKP-a za 2018. godinu planirana je izrada četiri smjernice, za 2019. godinu tri smjernice i za 2020. godinu preostale četiri smjernice. Odlukom VM-a MKP i MS su zaduženi da godišnje izvještavaju VM o realizaciji Politike upravljanja informacionom sigurnošću.

informacija iz upitnika, pregledom i analizom pravnih i strateških propisa u oblasti kibersigurnosti i drugih značajnih propisa, dostupnih analiza i pretraživanjem i izučavanjem podataka i stručne literature koji su od značaja za ovu studiju. Podaci prikupljeni pregledom i analizom dokumentacije o uspostavi kibersigurnosti institucija iz uzorka su međusobno uspoređivani.

1.5. Struktura izvještaja

U poglavlju jedan predstavljeni su motivi koji su opredijelili Ured za reviziju institucija BiH da provede reviziju učinka na temu kibersigurnost u institucijama BiH. Ovo poglavlje sadrži cilj, obim i ograničenja revizije, reviziona pitanja, kriterije revizije, te izvore i metode revizije.

Kroz drugo poglavlje daju se podaci i informacije nužne za razumijevanje kibersigurnosti, regulativnog okvira, strateškog opredjeljenja i uloge mjerodavnih institucija u oblasti kibersigurnosti.

U poglavlju tri predstavljeni su osnovni nalazi revizije do kojih se došlo provedenim istraživanjima. Poglavlje 3.1. nudi nalaze revizije koji ukazuju na nedostatak strateškog i zakonskog okvira za uspostavu kibersigurnosti u institucijama BiH, u poglavlju 3.2. prezentovani su nalazi koji ukazuju na nedostatak CERT-a u institucijama BiH, a u poglavlju 3.3. prezentovani su nalazi koji ukazuju na pasivan pristup institucija BiH u donošenju akata upravljanja informacionom sigurnošću.

Poglavlje četiri prezentuje zaključke revizije koji daju odgovor na reviziona pitanja.

Preporuke Ureda za reviziju institucija BiH čijim bi se provođenjem trebalo doprinijeti uspostavi kibersigurnosti u institucijama BiH date su u petom poglavlju.

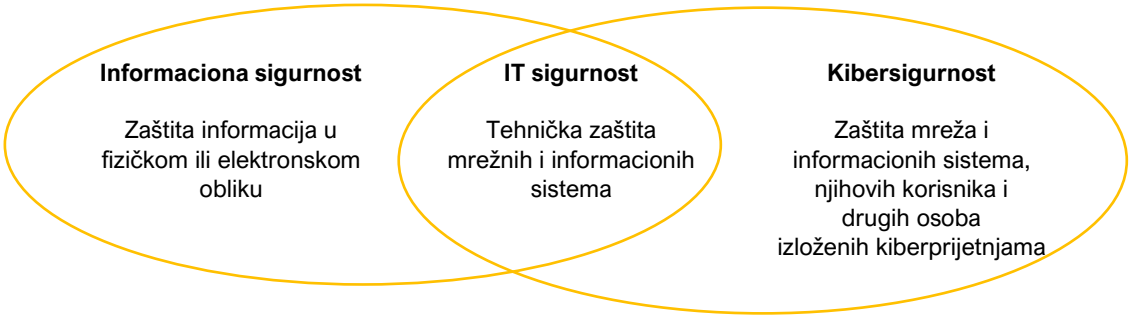
2. OPIS PREDMETA REVIZIJE

U ovom poglavlju predstavljeni su opći podaci bitni za razumijevanje kibersigurnosti, strateškog opredjeljenja za uspostavu kibersigurnosti, regulativnog okvira koji se odnosi na kibersigurnost u institucijama BiH i uloge mjerodavnih institucija BiH.

2.1. Kibersigurnost

Ne postoji općeprihvaćena, standardna definicija kibersigurnosti.[18] Kibersigurnost obuhvata sve aktivnosti koje su nužne za zaštitu od kiberprijetnji mrežnih i informacionih sistema, korisnika tih sistema i drugih osoba na koje one utiču. Kibersigurnost počiva na informacionoj sigurnosti. Informaciona sigurnost obuhvata aktivnosti kojima se postiže povjerljivost, cjelovitost i dostupnost informacija. Kibersigurnost obuhvata isto, ali u kiberprostoru. Zaštita mrežnih i informacionih sistema u kojima se informacije pohranjuju poznata je pod pojmom sigurnosti informacionih tehnologija (IT sigurnost) i predstavlja jedan dio informacione sigurnosti, odnosno kibersigurnosti koji se odnosi na tehničku zaštitu. Sljedeći grafikon prikazuje povezanost kibersigurnosti, informacione i IT sigurnosti.

Grafikon 1: Povezanost kibersigurnosti, informacione sigurnosti i IT sigurnosti



Izvor: Evropski revizorski sud

Kibersigurnost obuhvata prepoznavanje, sprečavanje i otkrivanje kiberincidenata[19], pružanje odgovora na njih i oporavak od njih. Uspostavom kibersigurnosti u institucijama BiH sprečavaju se različiti incidenti, od slučajnog do namjernog otkrivanja informacija i ličnih podataka, zastoja u radu i nedostupnosti sistema koji su podrška građanima i poslovnim korisnicima.

2.2. Strateško opredjeljenje za kibersigurnost

Početni koraci u izgradnji kibersigurnosti su ostvareni potpisivanjem Konvencije o kibernetičkom kriminalu 2006. godine i Sporazuma o stabilizaciji i pridruživanju 2008. godine. Na putu ka EU BiH je preuzela obaveze dostizanja određenih standarda u oblasti kibersigurnosti. Dvije najznačajnije regulative vezane za kibersigurnost na nivou EU su Direktiva o mjerama za visok zajednički nivo sigurnosti mrežnih i informacionih sistema

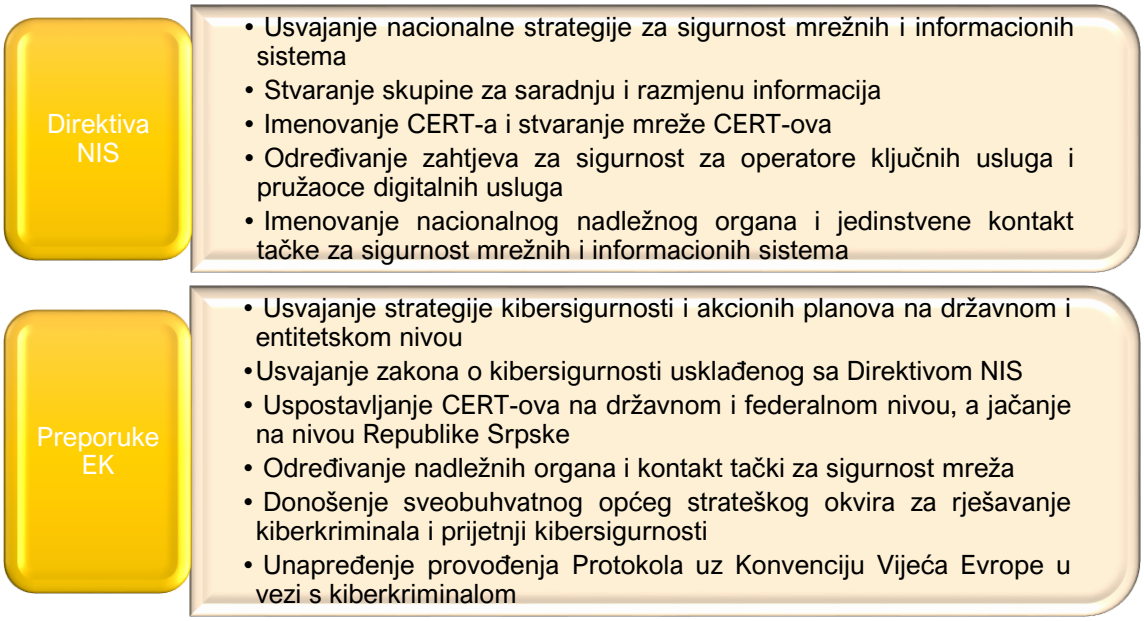
[18] Osim različitih definicija, postoje i različiti pojmovi kibersigurnosti. Kibernetička sigurnost je jedan od pojmova koji se poistovjećuje sa kibersigurnosti, iako postoje i različita tumačenja ova dva pojma. Ponekad se pojam kibersigurnosti poistovjećuje i sa informacionom sigurnošću.

[19] Kiberincident je događaj koji direktno ili indirektno narušava ili ugrožava otpornost i sigurnost IT sistema i podataka koji se obrađuju, pohranjuju ili prenose u okviru tog sistema.

širom Unije (Direktiva NIS),[20] donesena 2016. godine i Akt EU o kibersigurnosti,[21] donesen 2019. godine.

Usvajanjem preporuka EK, koje se upućuju BiH počev od 2016. godine, VM potvrđuje strateško opredjeljenje za uspostavu kibersigurnosti u institucijama BiH.[22] Sljedeći grafikon prikazuje preuzete obaveze u oblasti kibersigurnosti.

Grafikon 2: Preuzete obaveze u oblasti kibersigurnosti



Izvor: Ured za reviziju institucija BiH

Usvajanjem Akcionog plana 1 reforme javne uprave za period 2018 – 2022. godina, VM je podržao aktivnosti izrade zakonskih propisa zaštite informaciono-komunikacione infrastrukture i elektronskih usluga i uspostave CERT-a.[23]

Obaveze uspostavljanja CERT-a za institucije BiH i usvajanja kriterija za identifikaciju kritične infrastrukture institucija BiH i načina zaštite iste su potvrđene usvajanjem Finalnog izvještaja o realizaciji Akcionog plana za realizaciju prioriteta iz Analitičkog izvještaja EK za 2020. godinu.[24]

U Dodatku 1. izvještaja ilustriran je primjer susjedne zemlje Republike Hrvatske (RH) i način na koji je ona na svom putu ka EU i nakon što je postala članica EU uspostavljala strateški i zakonski okvir kibersigurnosti.

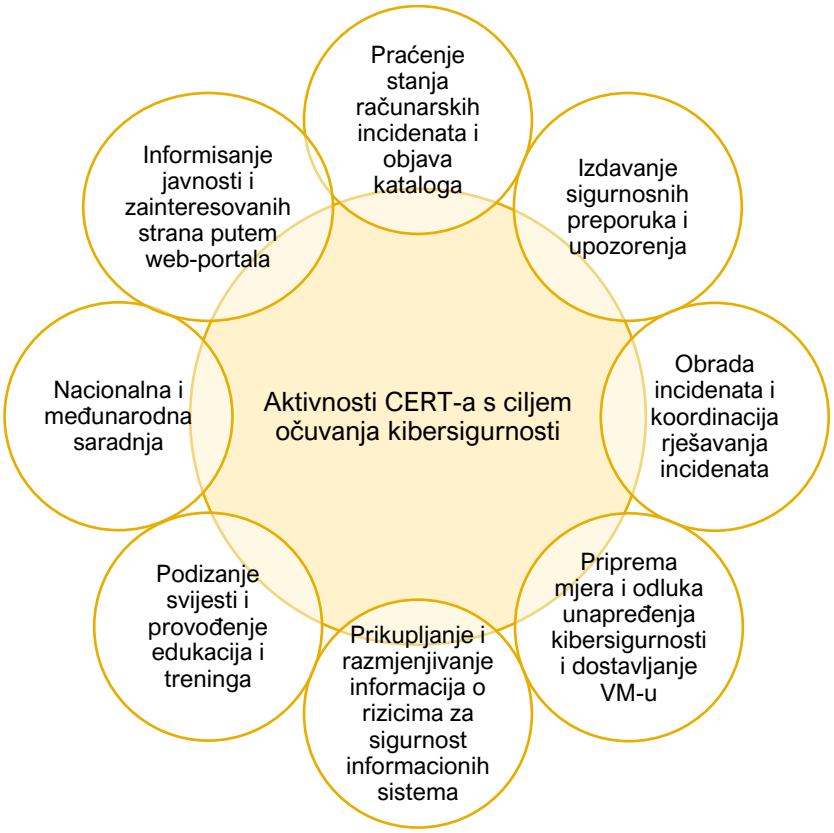
[20] Direktivom NIS utvrđuju se mjere s ciljem postizanja visokog zajedničkog nivoa sigurnosti mrežnih i informacionih sistema unutar EU kako bi se poboljšalo funkcionisanje unutrašnjeg tržišta.
[21] Aktom EU o kibersigurnosti nastoji se postići visok nivo kibersigurnosti, kiberotpornosti i povjerenja u EU utvrđivanjem ciljeva i zadaća Agencije EU za kibersigurnost i okvira za uspostavu dobrovoljnih evropskih programa kibersigurnosne certifikacije za proizvode, usluge i postupke informacione i komunikacione tehnologije. Aktom EU o kibersigurnosti se stavlja izvan snage Uredba iz 2013. godine o Agenciji EU za mrežnu i informacionu sigurnost.
[22] VM usvaja preporuke EK-a iz oblasti kibersigurnosti donesene na godišnjim sastancima Pododbora za pravdu, slobodu i sigurnost i Pododbora za inovacije, informaciono društvo i socijalnu politiku.
[23] Odgovorne institucije BiH (Služba za održavanje i razvoj elektronskog poslovanja i „e-vlade“ GS, MS i AZLP) su trebale realizovati aktivnosti do kraja 2022. godine.
[24] VM je usvojio Finalni izvještaj na 18. sjednici VM-a, održanoj 22. 10. 2020. godine.

2.3. Regulativni okvir za kibersigurnost u institucijama BiH

Na nivou institucija BiH ne postoji propis koji se isključivo bavi pitanjem kibersigurnosti i ovo pitanje djelimično je uređeno u okviru drugih propisa. Podzakonski propisi koji uređuju oblast kibersigurnosti u institucijama BiH su Odluka o određivanju CERT-a za institucije BiH[25] i Odluka o usvajanju Politike upravljanja informacionom sigurnošću[26]. Obje odluke djeluju u preventivnom smislu.

Odlukom o određivanju CERT-a za institucije BiH osigurava se koordinirano djelovanje za prevenciju i zaštitu od sigurnosnih rizika i smanjenju posljedica od sigurnosnih incidenata. Donošenjem Odluke o određivanju CERT-a za institucije BiH stvoreni su preduslovi za upravljanje kiberincidentima i jačanje kiberzaštite institucija BiH. Odlukom je određeno da se uspostavi CERT za institucije BiH u okviru MS-a. Sljedeći grafikon prikazuje planirane aktivnosti CERT-a za institucije BiH s ciljem očuvanja kibersigurnosti.

Grafikon 3: Aktivnosti CERT-a s ciljem očuvanja kibersigurnosti



Izvor: Ured za reviziju institucija BiH

Odlukom o usvajanju Politike upravljanja informacionom sigurnošću stvorena je osnova za uspostavu sistema za upravljanje informacionom sigurnošću u institucijama BiH u

[25] Sl. gl. BiH, broj 25/17. Odluka o određivanju CERT-a za institucije BiH određuje CERT u MS-u, odnosno Sektoru za informatiku i telekomunikacione sisteme, te definiše način djelovanja, modalitete i načine izvršavanja aktivnosti iz člana 6. Odluke, organizaciju i nadležnosti istog.

[26] Sl. gl. BiH, broj 38/17. Odlukom o usvajanju Politike upravljanja informacionom sigurnošću usvaja se Politika upravljanja informacionom sigurnošću koja definiše odnos organizacije prema informacionim dobrima i njena primarna svrha jeste da informiše rukovodioce, tehničke osobe i korisnike o bitnim zahtjevima za zaštitu informacione imovine, uključujući ljude, hardverske i softverske resurse i podatke.

skladu sa standardima za sigurnost informacionih sistema[27], izradu zakonskih i podzakonskih propisa i programa informacione sigurnosti. Uspostavom sistema upravljanja informacionom sigurnošću osiguravaju se svi aspekti zaštite nekog informacionog sistema i osigurava kvalitet uspostavljenih mjera informacione sigurnosti. Politikom upravljanja informacionom sigurnošću razvija se svijest o upravljanju informacionom sigurnošću i ukazuje na to da svaka institucija mora shvatiti neophodnost i potrebu realizovanja vlastite politike i uvođenja sistema za upravljanje informacionom sigurnošću. Za realizaciju Politike upravljanja informacionom sigurnošću određeni su MKP i MS.

2.4. Institucije BiH mjerodavne za kibersigurnost

Ministarstvo sigurnosti BiH

VM je odredio MS za uspostavu CERT-a, izradu Strategije kibersigurnosti i Zakona o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema. Poslovi u oblasti kibersigurnosti su dodijeljeni Sektoru za informatiku i telekomunikacione sisteme MS-a. Sektor za informatiku i telekomunikacione sisteme obavlja poslove na održavanju informatičke i mrežne opreme i druge poslove koje se odnose na informatičku i mrežnu opremu kao i poslove zaštite podataka u informacionom sistemu MS-a.[28]

Ministarstvo komunikacija i prometa BiH

VM je odredio MKP za izradu Zakona o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema i smjernica za izradu internih akata upravljanja informacionom sigurnošću. Poslovi na izradi Zakona i smjernica su dodijeljeni Sektoru za komunikacije i informatizaciju, tačnije Odsjeku za informatizaciju. Neki od poslova Sektora za komunikacije i informatizaciju su priprema analiza i drugih materijala, kao osnova za unapređenje politike razvoja sektora komunikacija i informatike, pripreme zakonskih i podzakonskih propisa u oblasti telekomunikacija i informatike i izrada propisa u oblasti informatike.[29]

[27] Standardi iz serije ISO 27000 (Sistem za upravljanje informacionom sigurnošću) institucijama pružaju smjernice za izradu, primjenu i provjeru sigurnosti informacionih sistema čime se osigurava povjerljivost, integritet i dostupnost informacionog sadržaja, sistema i procesa unutar institucije. Iako se u Politici upravljanja informacionom sigurnošću preporučuje upotreba standarda iz serije ISO 27000, u Politici upravljanja informacionom sigurnošću su navedeni i ostali međunarodno priznati standardi informacione sigurnosti.

[28] Prema Zakonu o ministarstvima i drugim organima uprave BiH (Sl. gl. BiH broj 5/03, 42/03, 26/04, 42/04, 45/06, 88/07, 35/09, 59/09, 103/09, 87/12, 6/13, 19/16 i 83/17) MS je, između ostalog, mjerodavan za sprečavanje i otkrivanje činilaca krivičnih djela terorizma, trgovine drogom, krivotvorenja domaćih i strane valute i trgovine ljudima i drugih krivičnih djela sa međunarodnim ili međuentitetskim elementom i prikupljanje i korištenje podataka od značaja za sigurnost BiH.

[29] Prema Zakonu o ministarstvima i drugim organima uprave BiH (Sl. gl. BiH broj 5/03, 42/03, 26/04, 42/04, 45/06, 88/07, 35/09, 59/09, 103/09, 87/12, 6/13, 19/16 i 83/17) MKP je, između ostalog, mjerodavan za pripremu i izradu strateških i planskih dokumenata u oblasti međunarodnih i međuentitetskih komunikacija, prometa, infrastrukture i informacionih tehnologija.

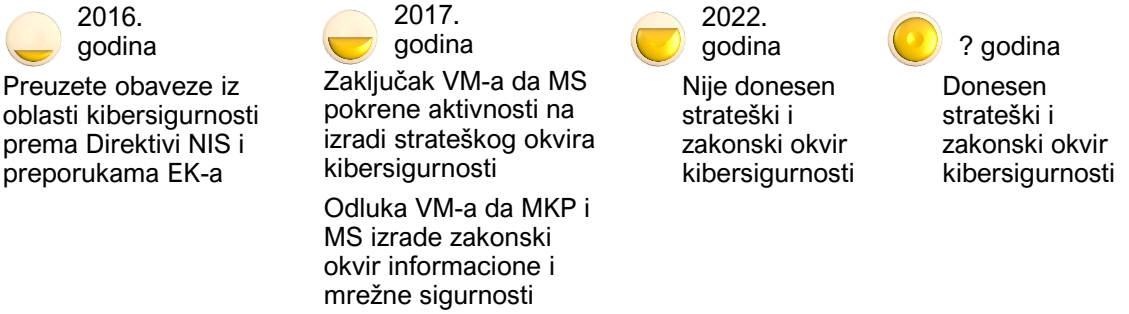
3. NALAZI REVIZIJE

U ovom poglavlju predstavljeni su nalazi revizije koji ukazuju na nedostatak osnovnih pretpostavki za izgradnju kibersigurnosti. Nalazi revizije su predstavljeni u tri poglavlja. U prvom poglavlju prezentovane su informacije o aktivnostima institucija BiH na donošenju strateškog i zakonskog okvira kibersigurnosti. U drugom poglavlju govorimo o aktivnostima formiranja CERT-a, a u trećem ćemo govoriti o aktivnostima institucija BiH na donošenju akata upravljanja informacionom sigurnošću.

3.1. Nedostatak strateškog i zakonskog okvira kibersigurnosti

U ovom poglavlju prezentovat ćemo nalaze revizije koji ukazuju na to da odgovorne institucije BiH nisu blagovremeno preduzimale aktivnosti na donošenju strateškog i zakonskog okvira kibersigurnosti. Aktivnosti na donošenju strateškog i zakonskog okvira kibersigurnosti pokrenute su još 2017. godine, a pet godina nakon toga aktivnosti nisu okončane i strateški i zakonski okvir kibersigurnosti još uvijek nije donesen. Sljedeći grafikon prikazuje tok uspostave obaveze donošenja strateškog i zakonskog okvira kibersigurnosti.

Grafikon 4: Tok uspostave obaveze donošenja strateškog i zakonskog okvira kibersigurnosti



Izvor: Ured za reviziju institucija BiH

Iz grafikona je vidljivo da ni nakon pet godina od zaduženja VM-a odgovorne institucije BiH nisu izradile strateški i zakonski okvir kibersigurnosti i izvjesno je da dinamika aktivnosti odgovornih institucija BiH neće osigurati završetak ovih aktivnosti u trenutno definisanom roku.[30]

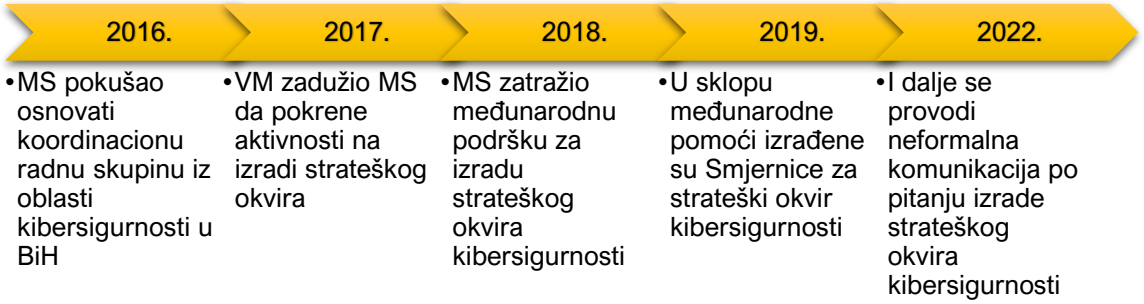
3.1.1. Nedostatak strateškog okvira kibersigurnosti

Za pet godina od kada je VM zadužio MS da preduzme aktivnosti na izradi strateškog okvira kibersigurnosti, MS nije uspio pripremiti strateški okvir kibersigurnosti koji bi VM usvojio.[31] Iako je VM 2017. godine zadužio MS da pokrene aktivnosti na izradi strateškog okvira, nije definisao rok niti način izvještavanja o realizaciji aktivnosti. Iako je VM naknadno definisao rokove za izradu strateškog okvira kibersigurnosti, MS nije u

[30] Trenutno definisani rok za izradu strateškog i zakonskog okvira kibersigurnosti je kraj 2022. godine.
[31] VM je na 107. sjednici, održanoj 6. 7. 2017. godine, usvojio Analizu o usklađenosti pravnih propisa u oblasti kibersigurnosti u BiH, koju je pripremio MS, i zadužio MS da intenzivira aktivnosti na izradi Strategije kibersigurnosti u BiH.

definisanim rokovima realizovao aktivnosti.[32] Sljedeći grafikon prikazuje aktivnosti MS-a na izradi strateškog okvira kibersigurnosti.

Grafikon 5: Aktivnosti MS-a na izradi strateškog okvira kibersigurnosti



Izvor: Ured za reviziju institucija BiH

Iz grafikona je vidljivo da je MS još 2016. godine pokušao osnovati radnu skupinu koja bi radila na izradi strateškog okvira kibersigurnosti, ali zbog nedostatka saglasnosti svih predstavnika entiteta, radna skupina nije osnovana. Narednih pet godina od zaduženja VM-a, MS nije pokušao osnovati radnu skupinu za izradu strateškog okvira. MS je tek nakon godinu dana od zaduženja VM-a preduzeo aktivnosti na izradi strateškog okvira i zatražio međunarodnu podršku. U sklopu međunarodne podrške osnovana je neformalna radna skupina za izradu strateškog okvira kibersigurnosti. Radna skupina zbog nedostatka saglasnosti svih članova nije izradila strateški okvir kibersigurnosti, već Smjernice za strateški okvir kibersigurnosti u BiH. Nije bilo drugih formalnih aktivnosti MS-a na izradi strateškog okvira kibersigurnosti. Prema izjavama predstavnika MS-a, vodi se neformalna komunikacija oko izrade strateškog okvira.

Trenutno, MS nije usaglasio i izradio model strateškog okvira kibersigurnosti prema preporukama EK-a, niti je pokušao izraditi prijedlog strateškog okvira za institucije BiH na osnovu Smjernica za strateški okvir kibersigurnosti u BiH.[33] MS nije izvještavao VM o kašnjenju u realizaciji aktivnosti na izradi strateškog okvira kibersigurnosti, osim za potrebe praćenja preporuka EK-a.[34]

Posljedica trenutnog stanja je nepostojanje jasno definisanih strateških ciljeva za izgradnju kibersigurnosti. Zbog nedostatka usaglašenog strateškog okvira kibersigurnosti, BiH značajno zaostaje u ispunjavanju preuzetih obaveza[35] i uređenju oblasti kibersigurnosti, zbog čega je narušen ugled institucija BiH.[36] Prema izjavama sagovornika mjerodavnih institucija BiH, zbog nedostatka strateškog okvira donatori

[32] VM je u 2019. i 2020. godini usvojio preporuke EK-a sa listom aktivnosti. Prvobitno je predloženi rok EK za izradu strateškog okvira kibersigurnosti u BiH bio 2020. godina, a zatim je prolongiran za 2021. godinu. MS je određen da vodi i koordinira aktivnosti na izradi strateškog okvira kibersigurnosti sa nadležnim institucijama BiH.

[33] Donesene Smjernice za strateški okvir kibersigurnosti u BiH predstavljaju početni korak u pravcu izgradnje kibersigurnosti i strateški okviri koji se izrade trebaju minimalno da sadrže navedene strateške ciljeve iz Smjernica za strateški okvir kibersigurnosti.

[34] MS je za potrebe praćenja preporuka EK-a navodio da nije usvojena strategija kibersigurnosti, da su aktivnosti na izradi i usaglašavanju modela strateškog dokumenta u skladu s Direktivom NIS i ustavnim uređenjem BiH u toku i da je ovo pitanje koje treba riješiti na političkom nivou.

[35] U prilog navedenom govori i činjenica da je nedavno objavljena nova Direktiva NIS, a BiH još uvijek nije implementirala obaveze iz prvotne direktive.

[36] Zajednička izjava većine predstavnika institucija iz uzorka, dok je veliki broj institucija BiH u popunjenom upitniku o kibersigurnosti naglasio da narušen ugled države i institucija BiH je moguća posljedica koja bi se desila u slučaju kibernapada ili računarskog incidenta.

smatraju da BiH ima neozbiljan pristup izgradnji kibersigurnosti zbog čega se manje sredstava ulaže u ovu oblast.

Nedostatak strateškog okvira doprinosi i zaostajanju u donošenju zakonskog okvira. O nedostatku zakonskog okvira govorimo u sljedećem poglavlju.

3.1.2. Nedostatak zakonskog okvira kibersigurnosti

Na nivou institucija BiH ne postoji zakonski okvir kojim se reguliše kibersigurnost, odnosno mrežna i informaciona sigurnost i nadležni organi, iako je donošenje zakonskog okvira planirano još od 2017. godine. Posljedice su nedostatak mjera i standarda informacione sigurnosti u institucijama BiH i nadležnih organa koji bi osigurali provođenje i nadzor mjera i koordinaciju u sprečavanju kiberincidenata. Ovo je jedan od uzroka niskog nivoa kibersigurnosti u institucijama BiH.

Odgovorne institucije BiH nisu izradile zakonski okvir kibersigurnosti u definisanim rokovima, iako je prošlo pet godina od zaduženja VM-a. VM je 2017. godine usvojio Politiku upravljanja informacionom sigurnošću i stvorio osnovu za donošenje Zakona o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema. Za izradu zakonskog okvira VM je odredio MKP i MS, ali nije odmah definisao rok za realizaciju aktivnosti. Rokovi su definisani naknadno, 2019. i 2020. godine. Sljedeći grafikon prikazuje aktivnosti MKP-a i MS-a na izradi zakonskog okvira kibersigurnosti.

Grafikon 6: Aktivnosti MKP-a i MS-a na izradi zakonskog okvira kibersigurnosti

Izvor: Ured za reviziju institucija BiH

Kao što je vidljivo iz grafikona, MKP i MS nisu blagovremeno i usaglašeno preduzimali aktivnosti na izradi zakonskog okvira kibersigurnosti. Jedan od razloga je različit pristup izradi zakonskog okvira kibersigurnosti i neusaglašeni stavovi oko načina implementacije Direktive NIS. Iako su za izradu zakonskog okvira određeni MKP i MS, aktivnosti je vodio MKP. MKP je tek nakon dvije godine od zaduženja VM-a preduzeo aktivnosti na osnivanju radne skupine. Iako je iste godine VM zadužio MKP da dostavi zakonski okvir na usvajanje do kraja 2019. godine, MKP nije vodio aktivnosti u sklopu radne skupine i izradio i

dostavio prijedlog zakonskog okvira VM-u.[37] Na taj način MKP i MS nisu realizovali aktivnosti u definisanim rokovima.

Ni u narednim godinama MKP i MS nisu uspjeli osnovati radnu skupinu za izradu zakonskog okvira niti su izradili zakonski okvir. Jedan od razloga zbog kojeg nije osnovana interresorna radna skupina za izradu zakonskog okvira u 2021. godini je nepostizanje saglasnosti svih predstavnika entiteta. MKP nije preduzimao dodatne aktivnosti na dobijanju saglasnosti entiteta niti je o navedenom problemu izvijestio VM. Na ovaj način nije iskorištena ni pružena međunarodna pomoć u izradi zakonskog okvira kibersigurnosti u skladu s Direktivom NIS zbog čega se kasni u ispunjavanju preuzetih obaveza. U datim okolnostima i zbog neusaglašenih stavova oko izrade zakonskog okvira sa MKP-om, MS samostalno priprema prijedlog zakonskog okvira.[38] Pripremljeni materijal još uvijek nije dobio formu konačnog prijedloga.[39]

MKP i MS nisu zajednički izvještavali VM o aktivnostima na izradi zakonskog okvira, iako je VM odredio MKP i MS da godišnje izvještavaju o realizaciji Politike upravljanja informacionom sigurnošću. Samo je MKP kroz redovno izvještavanje informisao VM da nije izrađen zakonski okvir. Nije bilo korektivnih aktivnosti VM-a na osnovu redovnog izvještavanja.

Nedostatak obavezujućih mjera i standarda informacione sigurnosti dovodi do većih rizika od kiberincidenata. U sljedećem poglavlju govorit ćemo o nedostatku organa za sprečavanje kiberincidenata.

3.2. Nedostatak Tima za odgovor na računarske incidente – CERT-a

U ovom poglavlju prezentovat ćemo nalaze revizije koji ukazuju na kašnjenje u uspostavi CERT-a za institucije BiH i mreže CERT-ova.

Na nivou institucija BiH, ni nakon pet godina od donošenja Odluke VM-a o određivanju CERT-a za institucije BiH, nije uspostavljen CERT koji bi učinkovito koordinirao i upravljao pružanjem odgovora na računarske incidente. Iako je VM zadužio MS da u kratkom roku preduzme aktivnosti s ciljem uspostave CERT-a za institucije BiH, MS za pet godina nije osigurao potrebne uslove za uspostavu CERT-a. Posljedice su nedostatak proaktivnih i reaktivnih mjera s ciljem očuvanja kibersigurnosti institucija BiH i smanjenja posljedica računarskih incidenata.[40] Zbog navedenog, institucije BiH su izložene većim sigurnosnim rizicima i kiberprijetnjama.

---

[37] VM je na 174. sjednici, održanoj 2. 7. 2019. godine, usvojio Informaciju o ispunjavanju pravnog kriterija institucija BiH i zadužio MKP da najdalje do kraja 2019. godine dostavi VM-u na usvajanje nacrt zakona o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema. Na istoj sjednici VM je usvojio preporuke EK-a i listu aktivnosti prema kojoj MKP i MS trebaju izraditi zakonski okvir kibersigurnosti usklađen sa Direktivom NIS do kraja 2019. godine. U 2020. godini rok je prolongiran do 2021 / 2022. godine.

[38] Aktivnosti na izradi zakona o mrežnoj i informacionoj sigurnosti institucija BiH MS je radio na osnovu Programa rada MS-a i VM-a za 2021. MS je pripremio ovaj zakon u saradnji sa UNDP-om. MS je mišljenja da se zakonski okvir kibersigurnosti može raditi samo za institucije BiH, a MKP smatra da se Direktiva NIS u potpunosti može implementirati samo na način da se radi zakonski okvir kibersigurnosti koji će obuhvatiti sve kritične infrastrukture u BiH.

[39] MS nije preduzeo aktivnosti na formiranju radne skupine za izradu zakonskog okvira, niti je pripremljeni materijal prošao procedure usklađivanja i pribavljanja mišljenja nadležnih institucija BiH.

[40] Proaktivnim mjerama se djeluje prije incidenta i drugih događaja koji mogu ugroziti sigurnost informacionih sistema, a u cilju sprečavanja ili ublažavanja mogućih šteta. Reaktivnim mjerama odgovara se na incidente te na druge događaje koji mogu ugroziti kibersigurnost informacionih sistema.

Kao prijelomni trenutak za detaljnu analizu aktivnosti uspostave CERT-a za institucije BiH uzeto je donošenje Odluke o određivanju CERT-a za institucije BiH 2017. godine, iako su aktivnosti na uspostavi CERT-a započele još 2011. godine. Sljedeći grafikon prikazuje tok uspostave CERT-a za institucije BiH.

Grafikon 7: Tok uspostave CERT-a za institucije BiH

Izvor: Ured za reviziju institucija BiH

Kao što je vidljivo iz grafikona, aktivnosti na uspostavi CERT-a su započele još 2011. godine kada je VM usvojio Strategiju uspostave CERT-a u BiH i donio Odluku o osnivanju i imenovanju ekspertne radne skupine za formiranje CERT tijela u BiH. Ekspertna radna skupina je izradila Akcioni plan uspostave BiH CERT-a koji nije usvojen na VM-u. To je bila zadnja aktivnost na uspostavi BiH CERT-a. Prema izjavama sagovornika iz MS-a, koji je vodio navedene aktivnosti, nije bilo podrške svih učesnika radne skupine za dalje aktivnosti na uspostavi BiH CERT-a. Narednih pet godina MS nije preduzimao aktivnosti na uspostavi CERT-a.

Naredna aktivnost na uspostavi CERT-a je preduzeta tek 2016. godine kada je VM usvojio Informaciju o aktivnostima MS-a u vezi sa kibersigurnosti.[41] VM je zadužio MS da izradi prijedlog odluke o određivanju CERT-a za institucije BiH, dostavi VM-u na usvajanje i izradi prijedloge odluka i akata unutrašnje organizacije kojima će osigurati okvir za CERT za institucije BiH. VM je 2017. godine donio Odluku o određivanju CERT-a za institucije BiH i zadužio MS da u roku od tri mjeseca predloži VM-u dopunu Pravilnika o unutrašnjoj organizaciji s ciljem uspostave CERT-a u MS-u.[42] MS nije u roku od tri mjeseca dostavio VM-u na usvajanje dopunu Pravilnika o unutrašnjoj organizaciji s ciljem uspostave CERT-a za institucije BiH. Sljedeći grafikon prikazuje aktivnosti MS-a s ciljem uspostave CERT-a (detaljniji pregled je u Dodatku 2.).

[41] Informacija je usvojena na 64. sjednici VM-a, održanoj 14. 7. 2016. godine.
[42] Određeno je da se uspostavi posebna unutrašnja organizaciona jedinica u okviru Sektora za informatiku i telekomunikacione sisteme MS-a.

Grafikon 8: Aktivnosti MS-a s ciljem uspostave CERT-a za institucije BiH

Izvor: Ured za reviziju institucija BiH

Kao što je vidljivo iz grafikona, MS-u je trebalo godinu dana da pošalje prvi nekompletni prijedlog dopuna Pravilnika o unutrašnjoj organizaciji u GS s ciljem uspostave CERT-a za institucije BiH. Iako je MS u 2018. godini u dva navrata dostavio GS-u nove prijedloge izmjena Pravilnika o unutrašnjoj organizaciji, materijali nisu bili predmet razmatranja na sjednicama VM-a zbog nedostajućih mišljenja.[43] Nakon što su pribavljena potrebna mišljenja, MS je 2019. godine dostavio materijal u GS. Materijal ni tada nije bio predmet razmatranja VM-a jer je GS tražio da se MS izjasni koji tačno materijal treba biti razmatran. Nakon toga MS povlači materijal iz dalje procedure i preduzima aktivnosti na izradi novog pravilnika o unutrašnjoj organizaciji i formira radnu skupinu za izradu novog pravilnika. Ni nakon pet godina MS u proceduru nije uputio kompletirani prijedlog pravilnika o unutrašnjoj organizaciji s ciljem uspostave CERT-a.

Trenutno nije poznato kada će MS izraditi prijedlog pravilnika o unutrašnjoj organizaciji i dostaviti VM-u.[44] S obzirom na to da nisu osigurani organizacioni preduslovi za uspostavu CERT-a, nije poznato ni kada će CERT postati operativan i obavljati dodijeljene poslove.[45] Iako MS kroz redovno izvještavanje informiše VM o kašnjenju u uspostavi CERT-a zbog neusvajanja izmjena Pravilnika o unutrašnjoj organizaciji, VM nije tražio dodatna pojašnjenja.

S obzirom na to da MS nije uspostavio CERT, nije osigurao ni preduslove za uspostavu mreže CERT-ova u BiH, zbog čega nije uspostavljena mreža CERT-ova.[46] Uspostavljanje CERT-a za institucije BiH i mreže CERT-ova su preuzete obaveze koje nisu ispunjene.

[43] Prijedlozi izmjena Pravilnika su osim za CERT, sublimirali i druge izmjene koje se ne odnose na CERT.

[44] Sektor za informatiku i telekomunikacije je u više navrata informisao Kabinet ministra o razlozima zbog kojih je potrebno pripremiti izmjene Pravilnika o unutrašnjoj organizaciji, odnosno donijeti novi pravilnik s ciljem uspostave CERT-a i izvršiti zapošljavanje u CERT. U 2022. godini su tražili od Sektora za pravne, kadrovske i opće poslove pokretanje procedure usvajanja izmjena Pravilnika o unutrašnjoj organizaciji s ciljem uspostave CERT-a. Na dostavljene informacije nije bilo konkretnih odgovora.

[45] Osim organizacionih preduslova, potrebno je osigurati i tehničke preduslove za CERT, što iziskuje dodatno vrijeme i sredstva. Prema izjavama sagovornika, nakon usvajanja prijedloga pravilnika o unutrašnjoj organizaciji potrebno je minimalno dvije godine da se osiguraju ostali preduslovi za operativnost CERT-a.

[46] Uspostavljanje državnog CERT-a ne sprečava uspostavu i drugih CERT-ova, štaviše, relevantne preporuke govore da svaka država treba uspostaviti više CERT-ova, za svako ključno područje. Prema dostupnim informacijama, u BiH je uspostavljen CERT Republike Srpske, CERT Ministarstva odbrane BiH i Akademski CERT. U Federaciji je CERT u fazi uspostavljanja.

MS nije uspostavio mrežu CERT-ova u definisanim rokovima.[47] Nedostatak mreže CERT-ova je jedan od razloga zašto nema registra ili kataloga kiberincidenata u BiH i pregleda upozorenja na potencijalne kiberprijetnje.

Nedostatak CERT-a doprinosi niskom nivou svijesti o važnosti očuvanja kibersigurnosti. U sljedećem poglavlju govorimo o nezadovoljavajućem nivou svijesti u institucijama BiH o važnosti očuvanja kibersigurnosti.

3.3. Pasivan pristup u donošenju akata upravljanja informacionom sigurnošću

U ovom poglavlju prezentovat ćemo nalaze revizije koji ukazuju na nedovoljan nivo kibersigurnosti, odnosno informacione sigurnosti u institucijama BiH.

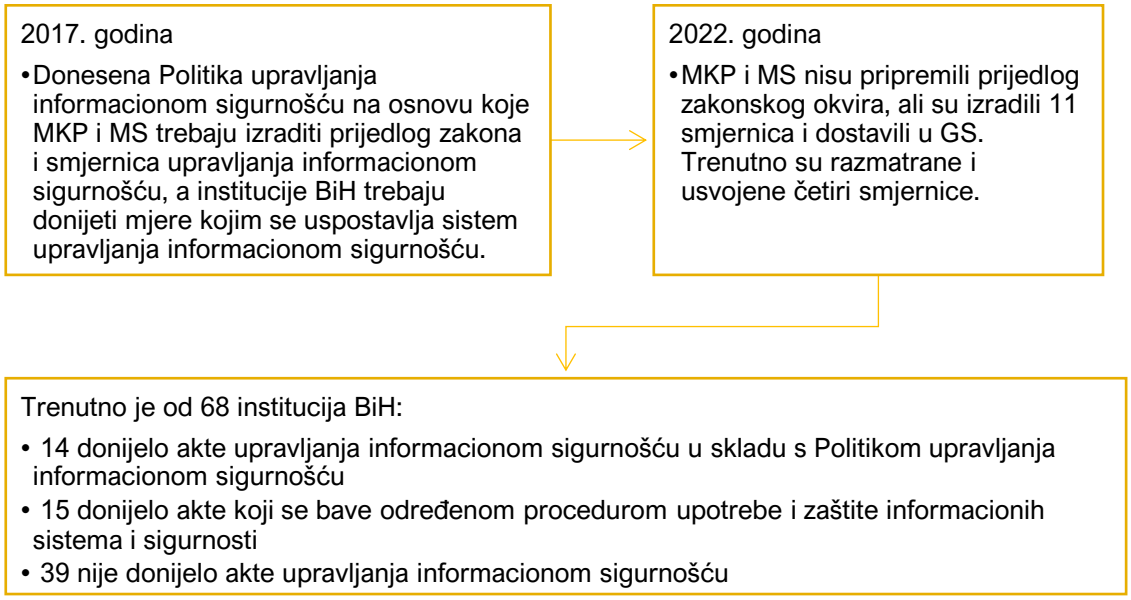
Institucije BiH su imale pasivan pristup u donošenju akata upravljanja informacionom sigurnošću u skladu s Politikom upravljanja informacionom sigurnošću i/ili standardima upravljanja informacionom sigurnošću.[48] Ni nakon pet godina od donošenja Politike više od polovine institucija BiH nije donijelo akte upravljanja informacionom sigurnošću. Neki od razloga pasivnog pristupa su nedostatak zakonskog okvira, neblagovremeno donošenje smjernica iz Politike upravljanja informacionom sigurnošću[49] i nedovoljan nivo svijesti o važnosti zaštite kibersigurnosti. Posljedice su slaba implementacija mjera i standarda informacione sigurnosti što dovodi do niskog nivoa informacione sigurnosti u institucijama BiH. Sljedeći grafikon prikazuje trenutno stanje realizacije Politike upravljanja informacionom sigurnošću.

[47] U listi aktivnosti EK-a za 2020. godinu rok za realizaciju osnivanja radne skupine za izradu Odluke o uspostavljanju mreže CERT-ova je prva polovina 2021. godine. U Programu rada MS-a za 2021. godinu planirana je izrada Odluke o uspostavljanju mreže CERT-ova u BiH.

[48] U Politici upravljanja informacionom sigurnošću preporučuje se izrada politike institucije, kao krovnog dokumenta, na osnovu koje će se izraditi ostali akti s ciljem uspostave sistema upravljanja informacionom sigurnošću.

[49] U Politici upravljanja informacionom sigurnošću opisano je 11 smjernica koje je potrebno izraditi, a to su: Smjernice o informatičkoj sigurnosti radnog mjesta, Smjernice o klasificiranju informacionih resursa, Smjernice o korištenju prijenosnih uređaja, Smjernice o fizičkoj zaštiti informacija, Smjernice o kontroli pristupa i bilježenju događaja, Smjernice o upravljanju sigurnosnim incidentima, Smjernice o upravljanju sigurnosnim zakrpama, Smjernice o korisničkim računima i pravima pristupa, Smjernice o sigurnosnim preslikama, Smjernice o zaposlenju i prekidu zaposlenja i Smjernice za izradu metodologije procjene rizika.

Grafikon 9: Dinamika realizacije Politike upravljanja informacionom sigurnošću



Izvor: Ured za reviziju institucija BiH

Kao što je vidljivo iz grafikona, tek nakon pet godina od donošenja Politike upravljanja informacionom sigurnošću VM je razmatrao i usvojio četiri smjernice iz Politike upravljanja informacionom sigurnošću.[50] Iako je MKP dostavio svih 11 smjernica u GS, predmet razmatranja je bio samo jedan set smjernica, dok preostala dva nisu. Iz razgovora sa predstavnikom MKP-a očekuje se usvajanje i preostalih smjernica na nekoj od idućih sjednica VM-a.

MKP je izradu smjernica podijelio u tri seta. Iako je prvi set smjernica izrađen još 2018. godine, a u naredne dvije godine i ostala dva seta smjernica, tek početkom 2022. godine su dostavljene u GS. Proces pribavljanja mišljenja MFT-a na smjernice je bio dugotrajan. Iako je MKP u više navrata pokušao organizovati sastanak sa predstavnicima MFT-a s ciljem dobijanja saglasnosti MFT-a, do 2022. godine nije osigurana saglasnost MFT-a, zbog čega smjernice nisu bile predmet ranijeg razmatranja na VM-u. Zbog neblagovremenog donošenja smjernica propuštena je prilika da institucije BiH pristupe izradi akata na osnovu smjernica iz Politike upravljanja informacionom sigurnošću.

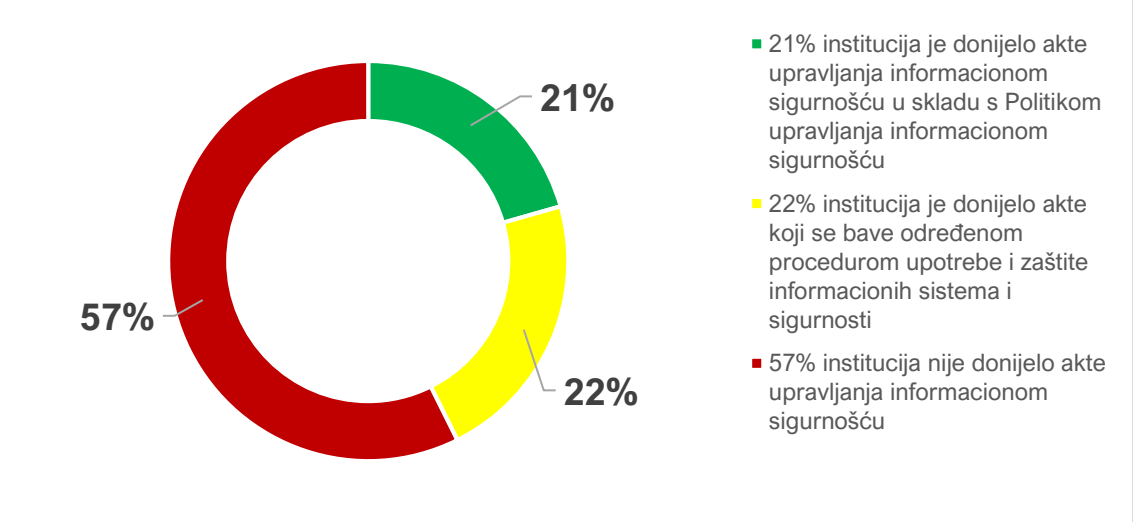
MKP i MS nisu izvještavali VM o slaboj realizaciji Politike upravljanja informacionom sigurnošću, iako ih je VM zadužio da vrše godišnje izvještavanje. MKP je u dva navrata putem godišnjih izvještaja o radu informisao VM o statusu smjernica iz Politike upravljanja informacionom sigurnošću. Nije bilo povratnih informacija nakon usvajanja izvještaja o radu MKP-a. MKP i MS nisu odredili način na koji bi pratili realizaciju Politike upravljanja informacionom sigurnošću u institucijama BiH, niti raspolažu informacijama o stanju u institucijama BiH.

U izostanku informacija o implementaciji Politike upravljanja informacionom sigurnošću, tim revizije je proveo ispitivanje u institucijama BiH i došao do podataka o trenutnom

[50] VM je na 54. sjednici, održanoj 28. 7. 2022. godine, donio Odluku o usvajanju smjernica iz Politike upravljanja informacionom sigurnošću i to četiri smjernice: Smjernice o korisničkim računima i pravima pristupa, Smjernice o sigurnosnim preslikama, Smjernice o zaposlenju i prekidu zaposlenja i Smjernice za izradu metodologije procjene rizika.

stanju.[51] Trenutno većina institucija BiH nije donijela akte upravljanja informacionom sigurnošću usklađene sa Politikom upravljanja informacionom sigurnošću i/ili međunarodnim standardima upravljanja informacionom sigurnošću, a što se vidi iz sljedećeg grafikona.

Grafikon 10: Trenutno stanje primjene Politike upravljanja informacionom sigurnošću u institucijama BiH



Izvor: Ured za reviziju institucija BiH

Kao što se vidi iz grafikona, većina institucija BiH nije donijela usklađene akte upravljanja informacionom sigurnošću, iako je od donošenja Politike upravljanja informacionom sigurnošću prošlo pet godina. Prema dostavljenim odgovorima samo 14 od 68 institucija BiH je donijelo usklađene akte upravljanja informacionom sigurnošću.[52] Od 68 institucija BiH 15 je donijelo akte koji se bave određenom procedurom upotrebe informaciono-komunikacionih sistema, a određeni broj institucija je detaljnije razradio mjere zaštite informaciono-komunikacionih sistema i sigurnosti informacija.[53]

Od 68 institucija BiH 39 nije donijelo akte upravljanja informacionom sigurnošću. Institucije su navodile različite razloge zašto nisu donijele navedene akte. Određeni broj institucija koji nije donio vlastite akte je na sistemu e-vlade i smatra da je e-vlada zadužena za sigurnost. Sličan primjer je i kod određenog broja pravosudnih institucija, koje su na informacionom sistemu Visokog sudskog i tužilačkog vijeća BiH. Određeni broj institucija BiH nije upoznat s Politikom upravljanja informacionom sigurnošću ili je mišljenja da im nije potrebno upravljanje informacionom sigurnošću za poslovanje.

[51] Provedeno je ispitivanje 73 institucije BiH, odgovore je dostavilo 68 institucija BiH na osnovu kojih je utvrđeno trenutno stanje. Revizioni tim je u pojedinim slučajevima obavljao telefonske razgovore radi pojašnjenja određenih odgovora u cilju prezentovanja što tačnijeg stanja. Bilo je manjih korekcija odgovora.
[52] Od 14 institucija koje su donijele akte upravljanja informacionom sigurnošću, određeni broj je izradio akte upravljanja informacionom sigurnošću i prije donošenja Politike upravljanja informacionom sigurnošću i izvršio certifikaciju sistema upravljanja informacionom sigurnošću.
[53] Prema dostavljenim odgovorima, 15 od 68 institucija BiH je donijelo akte upotrebe informaciono-komunikacionih sistema i/ili zaštite sigurnosti informacija ili određene procedure upotrebe informaciono-komunikacionih sistema, ali koji nisu usklađeni sa Politikom upravljanja informacionom sigurnošću i/ili međunarodnim standardima informacione sigurnosti.

Provođenjem revizije u institucijama iz uzorka uočen je različit stepen razvoja svijesti o važnosti upravljanja informacionom sigurnošću. Sljedeća tabela prikazuje trenutno stanje u institucijama iz uzorka.

Tabela 1: Trenutno stanje u institucijama iz uzorka

	Naziv institucije
Izrađeni akti upravljanja informacionom sigurnošću	AZLP i RAK
Akti upravljanja informacionom sigurnošću u izradi	MFT, MS i GS
Nisu izrađeni akti upravljanja informacionom sigurnošću	AJN i MKP
Broj ispitanih institucija	7

Izvor: Ured za reviziju institucija BiH

Kao što se vidi iz tabele 1. samo su dvije od sedam institucija iz uzorka donijele akte upravljanja informacionom sigurnošću u skladu sa Politikom upravljanja informacionom sigurnošću. AZLP je Opću politiku sigurnosti informacija donio 2017. godine. RAK je Politiku sigurnosti informacionog sistema donio 2019. godine.[54] Na sljedećoj ilustraciji prikazat ćemo primjer proaktivnog pristupa u uspostavi sistema upravljanja informacionom sigurnošću.

Ilustracija 1: Primjer proaktivnog pristupa u uspostavi upravljanja informacionom sigurnošću

AZLP je još 2014. godine započeo izgradnju sistema upravljanja informacionom sigurnošću u skladu sa ISO standardima informacione sigurnosti. Inicijativa je preduzeta nakon što je zabilježen kiberincident na web-stranicu što je dovelo do zastoja u radu od par sati. Inicijativa je preduzeta i prema preporukama Evropskog odbora za zaštitu ličnih podataka, s obzirom na to da se u informacionom sistemu AZLP-a nalaze registri ličnih podataka. Detaljne analize i koraci prema ISO standardu su urađeni sa angažovanom firmom. Opća politika sigurnosti informacija u skladu sa Politikom upravljanja informacionom sigurnošću je donesena 2017. godine, koju prati izrada ostalih pravila informacione sigurnosti. Dosada nije urađena certifikacija ISO standarda, ali je u planu.

Izvor: Ured za reviziju institucija BiH

Tri od sedam institucija iz uzorka su u fazi izrade akata upravljanja informacionom sigurnošću u skladu sa Politikom upravljanja informacionom sigurnošću. MFT i MS su nedavno pripremili nacrt akata upravljanja informacionom sigurnošću u skladu sa Politikom upravljanja informacionom sigurnošću, a GS je preduzeo početne aktivnosti na izradi. Iako su sve tri institucije mišljenja da nije dovoljan trenutni nivo informacione sigurnosti i da se treba unaprijediti, tek nakon pet godina od donošenja Politike informacione sigurnosti su preduzele aktivnosti na izradi.[55] Sve tri institucije kao jedan od razloga su navele nedostatak kadra.

Dvije od sedam institucija iz uzorka nisu donijele akte upravljanja informacionom sigurnošću. Obje institucije smatraju da se treba unaprijediti informaciona sigurnost, ali ni nakon pet godina od donošenja Politike upravljanja informacionom sigurnošću nisu izradile akte upravljanja informacionom sigurnošću. MKP nije pokrenuo aktivnosti jer je

[54] RAK je samostalno izradio politiku upravljanja informacionom sigurnošću u skladu sa Politikom upravljanja informacionom sigurnošću na osnovu koje su izvedeni ostali pravilnici i uputstva zaštite informacione sigurnosti. Analize koje su bile potrebne za izradu politike su rađene u skladu sa smjernicama iz Politike upravljanja informacionom sigurnošću.

[55] Sve tri institucije imaju određeni nivo zaštite informacione sigurnosti. U MFT-u se primjenjuju pravilnici za upotrebu i pristup informacionom sistemu MFT-a i procedure iz 2009. godine, 2010. godine i 2012. godine. U MS-u se primjenjuju Pravilnik o izradi sigurnosnih kopija i oporavak podataka iz 2013. godine i procedure pristupa Mrežnom operativnom centru MS-a iz 2018. godine i prema izjavi sagovornika druge procedure koje nisu generalizovane. GS primjenjuje Pravilnik o upotrebi zajedničkog informaciono-komunikacionog sistema u VM-u iz 2013. godine.

čekao donošenje smjernica, iako je MKP izradio nacrt smjernica.[56] AJN nije preduzimao aktivnosti jer nije bio upoznat s Politikom upravljanja informacionom sigurnošću.[57]

Većina institucija iz uzorka je imala zabilježenu određenu vrstu kiberincidenata. Od sedam institucija iz uzorka pet je imalo zabilježene kiberincidente na web-stranicu, elektronsku poštu i incidente kod provajdera. Na primjeru institucija iz uzorka ilustrirat ćemo posljedice zabilježenih kiberincidenata i druge moguće posljedice koje su istaknute na razgovorima u institucijama BiH.

Ilustracija 2: Istaknute posljedice i moguće posljedice u institucijama iz uzorka

Na osnovu razgovora u institucijama iz uzorka zabilježeni kiberincidenti prouzrokovali su obustavu rada od nekoliko sati do par dana, nedostupnost web-stranice i elektronske pošte. Posljedice za institucije su bile ugrožavanje kibersigurnosti, neovlašten pristup informacijama, gubitak radnih sati i povećanje troškova na oporavku informacionog sistema, kašnjenje u obavljanju poslova iz nadležnosti, gubitak povjerenja i narušen ugled institucije. Posljedice za korisnike usluga institucija su nemogućnost pristupa važnim informacijama, kao što su npr. javni pozivi za javne nabavke ili neblagovremena plaćanja iz budžeta. Sve institucije iz uzorka su mišljenja da bi u slučaju ostvarenog kibernapada posljedice bile značajnije, od ugrožavanja sigurnosti, pouzdanosti i cjelovitosti podataka, oštećenja informacionog sistema, oštećenja ili trajnog gubitka podataka, ugrožavanja lične sigurnosti i sigurnosne situacije i funkcionisanja zemlje, narušene reputacije i odbijanje potencijalnih investitora.

Izvor: Ured za reviziju institucija BiH

Slaba primjena mjera i standarda informacione sigurnosti dovodi do ugrožavanja kibersigurnosti i može dovesti do značajnih posljedica. Iako revizija nije detaljno analizirala primjenu mjera uočeno je da postoje određene slabosti u primjeni osnovnih mjera informacione sigurnosti. Jedan od primjera je neodgovarajuća primjena lozinki za informacioni sistem.[58]

[56] Trenutno, MKP nema vlastite procedure već primjenjuju procedure e-vlade za upotrebu zajedničkog informaciono-komunikacionog sistema u VM-u.

[57] AJN je 2008. godine donio Odluku o upotrebi računara i zaštite podataka u 2008. godini i 2016. godine Interne i eksterne procedure backup-a.

[58] Naziv institucije ne navodimo da tu instituciju dodatno ne bismo izložili mogućnostima zloupotrebe.

4. ZAKLJUČCI REVIZIJE

Ured za reviziju institucija BiH proveo je reviziju učinka s ciljem da provjeri jesu li institucije BiH efikasne u preduzimanju aktivnosti u osiguranju osnovnih pretpostavki za kibersigurnost. Provedena istraživanja, intervjui i analiza relevantne dokumentacije omogućili su nam da sagledamo postojeće stanje te da iznesemo sljedeći zaključak.

Institucije BiH nisu efikasne u preduzimanju aktivnosti s ciljem osiguranja osnovnih pretpostavki za kibersigurnost. Na nivou institucija BiH nije osiguran strateški i zakonski okvir kibersigurnosti, niti je uspostavljen CERT za institucije BiH. Pojedinačne institucije BiH nisu bile efikasne u donošenju akata upravljanja informacionom sigurnošću u skladu sa Politikom upravljanja informacionom sigurnošću. Posljedice nedostatka osnovnih pretpostavki za kibersigurnost ugrožavaju poslovanje javne uprave i mogu dovesti do otuđenja podataka i finansijskih sredstava neophodnih za funkcionisanje zemlje i svakodnevnog života građana.

4.1. Nije osiguran strateški i zakonski okvir kibersigurnosti

Na nivou institucija BiH značajno se kasni u uspostavi strateškog i zakonskog okvira kibersigurnosti. Neblagovremeno definisanje rokova za realizaciju aktivnosti je pridonijelo slaboj realizaciji aktivnosti. Zbog nepostojanja strateškog i zakonskog okvira nisu osigurane osnovne pretpostavke za sistemsku izgradnju kibersigurnosti što je doprinijelo niskom nivou kibersigurnosti.

Odlaganje donošenja i usklađivanja strateškog i zakonskog okvira kibersigurnosti sa zakonodavstvom EU za posljedicu nema samo neispunjavanje preuzetih obaveza, već doprinosi tehnološkom zaostajanju institucija BiH. Tehnološko zaostajanje čini institucije BiH izloženijim većim sigurnosnim rizicima i prijetnjama što otežava digitalnu transformaciju javne uprave. Bez kibersigurnosti nije moguće uspostaviti digitalnu javnu upravu koja će pružati elektronske usluge i koja će pridonijeti ostvarivanju pristupa jedinstvenom digitalnom tržištu.

Izrada strateškog okvira kibersigurnosti je izazov na koji MS nije blagovremeno odgovorio i bez osigurane podrške nije mogao ponuditi najbolje moguće rješenje, uvažavajući kompleksno uređenje BiH. Bez strateškog okvira nije moguće uspostaviti koordinirani i planski pristup izgradnji kibersigurnosti, a bez takvog pristupa je teško osigurati kiberzaštitu informacionih sistema i mreža institucija BiH i njenih poslovnih subjekata i građana. Zbog nedostatka strateškog okvira donatori smatraju da BiH ima neozbiljan pristup izgradnji kibersigurnosti zbog čega manje sredstava ulažu u ovu oblast.

MKP i MS nisu zajednički pristupili pripremi zakonskog okvira kibersigurnosti i nisu ponudili najbolje moguće rješenje u datim okolnostima. Zakonski okvir kibersigurnosti nije donesen, što je uticalo na slabu implementaciju mjera i standarda informacione sigurnosti u institucijama u BiH. Slaba implementacija mjera dovodi do većih rizika i ranjivosti na kiberprijetnje. U takvim situacijama koriste se informacioni i mrežni sistemi koji nemaju odgovarajući nivo zaštite, a finansijska sredstva i podaci koji pripadaju institucijama BiH su lakše dostupni za nezakonito korištenje.

4.2. Nije uspostavljen CERT za institucije BiH

Na nivou institucija BiH značajno se kasni u uspostavi CERT-a za institucije BiH u odnosu na definisani rok. Zbog kašnjenja MS-a u osiguravanju potrebnih uslova nije uspostavljen CERT i nije osiguran koordinirani pristup u upravljanju pružanjem odgovora na kiberincidente. U izostanku koordiniranog pristupa nisu implementirane proaktivne i reaktivne mjere kibersigurnosti u institucijama BiH. Na taj način nije dostignut odgovarajući nivo kiberpripravnosti razmjeran kiberprijetnjama.

Neformiranjem CERT-a odgovorna institucija BiH nije osigurala uslove za uspostavu mreže CERT-ova zbog čega nema evidencija o kiberincidentima niti razmjene informacija i sigurnosnih preporuka. U nedostatku CERT-a nisu osigurana sigurnosna upozorenja i preporuke za pružanje odgovora na kiberincidente zbog čega su informacioni i mrežni sistemi institucija BiH podobniji za realizaciju kiberprijetnji. Svaki zabilježeni kibernapad narušava ugled institucija BiH i bez odgovarajućeg pruženog odgovora čini veću i dugotrajniju štetu po institucije BiH.

4.3. Neefikasno donošenje akata upravljanja informacionom sigurnošću

Većina institucija BiH nije imala proaktivan pristup u donošenju akata upravljanja informacionom sigurnošću u skladu s Politikom upravljanja informacionom sigurnošću. Neke od institucija BiH nisu ni bile upoznate s tim da postoji Politika, a neke smatraju da im nije potrebno upravljanje informacionom sigurnošću za poslovanje. MKP i MS nisu pratili implementaciju Politike upravljanja informacionom sigurnošću u institucijama BiH i na taj način upoznali i aktivirali institucije BiH sa Politikom. Nizak nivo svijesti o važnosti kibersigurnosti je možda i najviše uticao na pasivan pristup donošenju usklađenih akata upravljanja informacionom sigurnošću. Tako je propuštena prilika da institucije BiH postignu odgovarajući nivo zaštite informacione sigurnosti koja je normirana i potrebna za sigurno i učinkovito poslovanje.

Implementacija preventivnih mjera informacione sigurnosti u institucijama BiH nije dosljedna zbog čega nije ostvaren zadovoljavajući nivo kibersigurnosti. Institucije BiH zbog toga mogu biti podobnije za ugrožavanje kibersigurnosti što dovodi do značajnih posljedica i to ne samo za institucije, već za cijelu zemlju. Motiv za izgradnju kibersigurnosti potrebno je zasnivati na svijesti institucija BiH o važnosti zaštite kibersigurnosti, a ne na zaključcima međunarodnih izvještaja. Bez kibersigurnosti nema ni tehnološkog napretka BiH, a može biti i ograničen ekonomski napredak.

5. PREPORUKE REVIZIJE

Na osnovu provedenih istraživanja, nalaza i zaključaka revizije, Ured za reviziju daje sljedeće preporuke:

Preporuka Vijeću ministara BiH:

- **Definisati rokove za pripremu i odgovornost za izvještavanje o procesu pripreme relevantnih akata kibersigurnosti.**

VM svojim zaključkom može definisati rokove i odgovornost za izvještavanje o procesu pripreme relevantnih akata kibersigurnosti. Utvrđivanje rokova za izradu, jasnih odgovornosti i obaveze izvještavanja o procesu izrade propisa i ostalih akata kibersigurnosti omogućit će VM-u lakši nadzor nad ovim procesom i potaći će efikasnost odgovornih institucija.

Preporuke Ministarstvu komunikacija i prometa BiH i Ministarstvu sigurnosti BiH:

- **Žurno okončati pripremu prijedloga relevantnih propisa kibersigurnosti i dostaviti ih VM-u na usvajanje.**

Odgovorna ministarstva trebaju ubrzati aktivnosti na pripremi usaglašenog i prihvatljivog prijedloga zakonodavnog okvira. S tim u vezi potrebno je okončati aktivnosti formiranja odgovorne radne skupine ili preduzeti druge potrebne aktivnosti koje će dovesti do prihvatljivog prijedloga zakonskog okvira koji će regulisati kibersigurnost, odnosno informacionu sigurnost u institucijama BiH.

- **Izvijestiti VM o realizaciji Politike upravljanja informacionom sigurnošću u institucijama BiH.**

S ciljem unapređenja kibersigurnosti, odnosno informacione sigurnosti u institucijama BiH, odgovorna ministarstva trebaju izvijestiti VM o realizaciji Politike upravljanja informacionom sigurnošću i stanju u institucijama BiH. Odgovorna ministarstva se trebaju dogovoriti o načinu izvještavanja.

Preporuke Ministarstvu sigurnosti BiH:

- **Žurno okončati pripremu prijedloga strateškog okvira kibersigurnosti i dostaviti ga VM-u na usvajanje.**

Odgovorno ministarstvo treba ubrzati aktivnosti na pripremi usaglašenog i prihvatljivog prijedloga strateškog okvira. S tim u vezi potrebno je okončati aktivnosti formiranja odgovorne radne skupine ili preduzeti druge potrebne aktivnosti koje će dovesti do prihvatljivog prijedloga strateškog okvira koji će regulisati kibersigurnost, odnosno informacionu sigurnost u institucijama BiH.

- **Žurno osigurati organizacione pretpostavke za formiranje Tima za odgovor na računarske incidente za institucije BiH.**

Ovo može podrazumijevati da MS osigura organizacione pretpostavke kroz izmjenu relevantnih akata ministarstva ili donese druge odluke kojim će se osigurati organizacione pretpostavke za formiranje Tima za odgovor na računarske incidente za institucije BiH i dostavi VM-u na usvajanje.

Preporuka institucijama BiH:

- **Žurno donijeti akte upravljanja informacionom sigurnošću u skladu s Politikom upravljanja informacionom sigurnošću.**

S ciljem unapređenja informacione sigurnosti i uspostave sistema upravljanja informacionom sigurnošću, institucije BiH koje nisu izradile akte usklađene sa Politikom upravljanja informacionom sigurnošću trebaju izraditi akte na osnovu smjernica i standarda informacione sigurnosti iz Politike upravljanja informacionom sigurnošću.

Tim revizije učinka:

Magdalena Pejak
Viši revizor učinka - vođa tima

v.r.

Danijel Čolo
Rukovodilac Odjela za reviziju učinka

v.r.

Jasmina Zuko
Samostalni revizor učinka - član tima

v.r.

Radivoje Jeremić
Rukovodilac Odjela za kontrolu kvaliteta, metodologiju i planiranje revizije učinka

v.r.

DODACI

Dodatak 1. Ilustracija primjera susjedne zemlje Republike Hrvatske

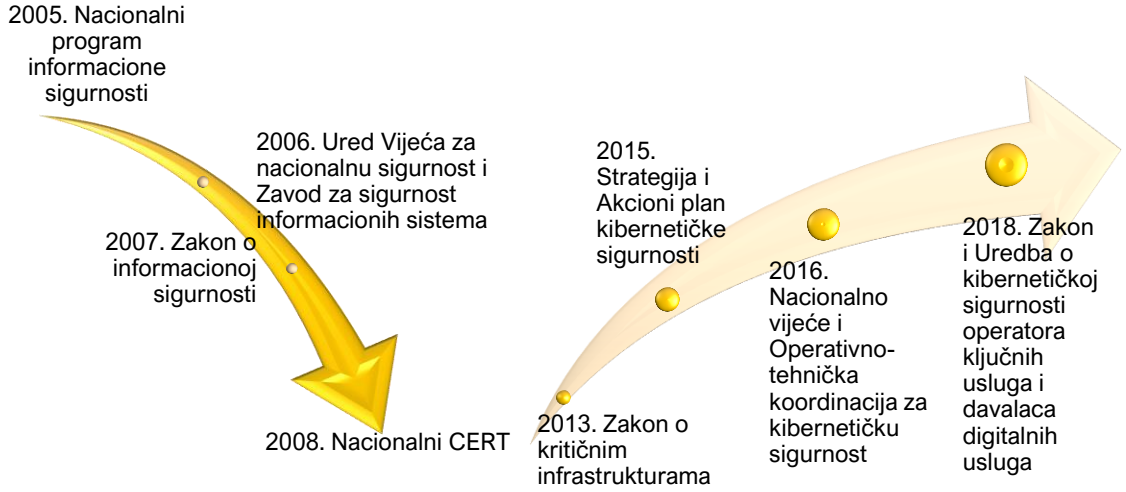
Dodatak 2. Hronologija aktivnosti Ministarstva sigurnosti BiH na izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji i pripreme novog Pravilnika o unutrašnjoj organizaciji

Dodatak 3. Reference

Dodatak 1. Ilustracija primjera susjedne zemlje Republike Hrvatske

RH ima razrađen zakonski i organizacioni okvir kibersigurnosti. Kao zemlja članica EU i Sjevernoatlantskog saveza (NATO), RH je implementirala zakonodavstvo EU i NATO-a u oblasti kibersigurnosti. Sljedeći grafikon prikazuje vremenski tok uspostave krovnog okvira kibersigurnosti u RH.

Grafikon 11: Uspostava okvira kibersigurnosti u RH



Izvor: Ured za reviziju institucija BiH

Informaciona sigurnost u RH je regulisana Nacionalnim programom informacione sigurnosti i Zakonom o informacionoj sigurnosti.[59] Navedena regulativa je stvorila osnovu za implementaciju mjera i standarda informacione sigurnosti u RH i organizacioni ustroj. Prema tome, organi državne uprave, lokalne i područne samouprave te pravne osobe s javnim ovlastima koje su vlasnici neklasifikovanih informacionih sistema u RH, dužni su donijeti opći akt upravljanja informacionom sigurnošću, odrediti odgovorne osobe za upravljanje informacionom sigurnošću, osigurati provođenje propisanih minimalnih mjera informacione sigurnosti u skladu s normama za upravljanje informacionom sigurnošću Međunarodne organizacije za standardizaciju (ISO) 27001 i uspostaviti kanale komunikacije sa organima nadležnim za prevenciju i koordinaciju odgovora na računarsko-sigurnosne incidente.

Djelovanje u području informacione sigurnosti je dodatno ojačano i prošireno donošenjem Strategije i Akcionog plana kibernetičke sigurnosti. Donošenjem Strategije kibernetičke sigurnosti, RH je sistemski pristupila provođenju aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora u skladu sa Direktivnom NIS. Stvorena je i osnova za donošenje Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davalaca digitalnih usluga, kojim je osigurano provođenje mjera za postizanje visokog zajedničkog nivoa kibernetičke sigurnosti u davanju usluga koje su od posebna važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti, uključujući funkcionisanje digitalnog tržišta. [60]

[59] Dodatno, podzakonski propisi koji regulišu informacionu sigurnost u RH su Uredba o mjerama informacione sigurnosti, Smjernice za postupanje s neklasifikovanim podacima i Pravilnik o standardima sigurnosti neklasifikovanih informacionih sistema.

[60] Donesena je i Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davalaca digitalnih usluga.

Djelovanje u prevenciji i zaštiti od računarskih incidenata RH je organizaciono podijelila između dva tijela, Nacionalnog CERT-a i Zavoda za sigurnost informacionih sistema. Ova dva tijela sarađuju i razmjenjuju informacije. Učestvuju u članstvu međunarodnih i evropskih organizacija u oblasti kibersigurnosti. Sarađuju i sa Nacionalnim vijećem za kibernetičku sigurnost, odnosno Uredom Vijeća za nacionalnu sigurnost u čijem su sastavu, koji djeluje kao jedinstvena nacionalna kontaktna tačka.

Nacionalni CERT je nacionalno tijelo za prevenciju i zaštitu od računarskih prijetnji sigurnosti javnih informacionih sistema u RH, čiji je osnovni zadatak obrada računarsko-sigurnosnih incidenata s ciljem očuvanja kibernetičke sigurnosti u RH. Nacionalni CERT se bavi i incidentima sa značajnim učinkom prema Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davalaca digitalnih usluga za sektore bankarstva, infrastrukture finansijskog tržišta, digitalne infrastrukture, dio poslovnih usluga za državne organe i davaoce digitalnih usluga.

Zavod za sigurnost informacionih sistema je centralni državni organ za prevenciju i zaštitu od računarskih prijetnji informacionih sistema državnih tijela RH i obavljanje poslova u tehničkim područjima informacione sigurnosti državnih tijela, koji obuhvataju standarde sigurnosti informacionih sistema, sigurnosnu akreditaciju informacionih sistema i upravljanje kriptomaterijalima koji se koriste u razmjeni klasifikovanih podataka.

Pored navedenog okvira, postoje i drugi zakonski i podzakonski propisi i organi koji su važni za informacionu sigurnost u RH koje zbog obimnosti nismo navodili.[61]

[61] Neki od zakonskih propisa koji su važni za informacionu sigurnost u RH su Zakon o tajnosti podataka, Zakon o zaštiti osobnih podataka, Zakon o elektroničkoj ispravi, Zakon o sigurnosnim provjerama, Zakon o sigurnosno-obavještajnom sustavu, Kazneni zakon i ostali zakonski i podzakonski propisi. Ostale institucije informacione sigurnosti u RH su Akademska i istraživačka mreža, Agencija za podršku informacijskim sustavima i informacijskim tehnologijama, Agencija za zaštitu osobnih podataka i Središnji državni ured za e-upravu.

Dodatak 2. Hronologija aktivnosti Ministarstva sigurnosti BiH na izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji i pripreme novog pravilnika o unutrašnjoj organizaciji

15. 7. 2016. godine GS prema MS	Obavijest o zaključku VM-a: VM usvojio Informaciju o aktivnostima MS-a u vezi sa kibersigurnosti i s tim u vezi, između ostalog, zadužio MS da izradi prijedloge odluka i akata unutrašnje organizacije radi osiguravanja okvira za BiH CERT za institucije BiH.
8. 3. 2017. godine VM usvojio Odluku o određivanju CERT-a za institucije BiH	U cilju realizacije Odluke, MS će u roku od tri mjeseca, od dana donošenja ove Odluke, predložiti VM-u dopunu postojećeg Pravilnika o unutrašnjoj organizaciji br. 01-02-125/08 od 9. 4. 2009. godine, s ciljem uspostavljanja posebne unutrašnje organizacione jedinice u okviru Sektora za informatiku i telekomunikacione sisteme MS-a.
19. 4. 2017. godine Pomoćnik ministra za informatiku i telekomunikacione sisteme prema Kabinetu ministra	Predmet: Informacija o potrebi izmjene i dopune Pravilnika o unutrašnjoj organizaciji MS-a radi realizacije zaključka VM-a i uspostavljanja CERT-a za institucije BiH: Predmetne izmjene i dopune treba da obuhvate izmjenu naziva i opisa poslova Sektora za informatiku i telekomunikacione sisteme, postojećih unutrašnjih organizacionih jedinica – odsjeka, te pojedinih izvršilaca u Sektoru. Također, potrebno je uvođenje novog odsjeka u okviru Sektora, tj. Odsjeka za CERT i sigurnost IKT sistema i povećanje broja izvršilaca u Sektoru.
12. 6. 2017. godine MS prema Ministarstvu pravde	Predmet: Prijedlog opisa poslova službeničkih radnih mjesta, mišljenje, traži se: Traži se mišljenje na opis poslova službeničkih radnih mjesta razvrstanih u kategorije (radna mjesta: sistem inženjeri, projektant programeri, stručni savjetnici, administratori IKT, itd.).
12. 9. 2017. godine MS prema Ministarstvu pravde	Predmet: Hitno dostavljanje mišljenja na prijedlog opisa poslova službeničkih radnih mjesta: Traži se mišljenje na opis poslova službeničkih radnih mjesta razvrstanih u kategorije. Isti akt kao 12. 6. 2017. godine.
9. 10. 2017. godine MS prema Ministarstvu pravde	Predmet: Hitno dostavljanje mišljenja na prijedlog opisa poslova službeničkih radnih mjesta (isto kao 12. 6. 2017. i 12. 9. 2017. godine).
23. 10. 2017. godine MS prema MFT-u	Predmet: Pravilnik o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, mišljenje, traži se: Izmjenama u pravilnik uvode novi Odsjek za CERT u okviru Sektora za informatiku i telekomunikacione sisteme, dopuna opisa poslova i opisi radnih mjesta u Sektoru.
MS prema Ministarstvu pravde	Predmet: Pravilnik o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, mišljenje, traži se;
MS prema Uredu za zakonodavstvo	Predmet: Pravilnik o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, mišljenje, traži se;
01. 11. 2017. godine Ured za zakonodavstvo prema MS-u	Predmet: Mišljenje na Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji: Ured za zakonodavstvo ukazuje MS-u da je potrebno da pribavi mišljenja od MP-a i MFT-a. Istovremeno ukazuje na obavezu donošenja novih pravilnika, te na obavezu iz člana 41. Aneksa i Metodologije procjene uticaja prilikom izrade propisa Jedinstvenih pravila za izradu pravnih propisa u institucijama BiH.
16. 11. 2017. godine Ministarstvo pravde prema MS-u	Predmet: Mišljenje na opis poslova radnih mjesta: MP daje pozitivno mišljenje i konstatuje da je prijedlog poslova svih 10 radnih mjesta pravilno sastavljen.
22. 11. 2017. godine Ministarstvo pravde prema MS-u	Predmet: Mišljenje na Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji: MP je mišljenja da bi opravdanost formiranja novog sektora trebalo preispitati s aspekta nadležnosti MS-a.

8. 12. 2017. godine MS prema MFT-u	Predmet: Pravilnik o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, mišljenje, traži se: Izvršene korekcije koje se odnose na zaposlenička radna mjesta u Sektoru za informatiku i telekomunikacione sisteme, te popunjen obrazac za razvrstavanje radnih mjesta srednje stručne spreme u platne razrede za radno mjesto 10. 18. Tehničar za sigurnost IKT sistema – referent specijalista.
11. 01. 2018. godine MS prema MFT-u	Predmet: Pravilnik o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, dopuna, dostavlja se: Vrše dopunu sa obrascem broj 2a o fiskalnoj procjeni uticaja, a koji se odnosi na spomenuti pravilnik.
13. 4. 2018. godine MS prema MFT-u	Predmet: Urgencija na davanje Mišljenja na Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, traži se: Aktom od 13. 2. 2018. godine MS je dostavio objedinjen tekst Prijedloga pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a da MFT na isti da svoje mišljenje.
13. 4. 2018. godine MS prema GS-u	Predmet: Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, dostavlja se: U prilogu akta dostavljaju mišljenja nadležnih institucija, s obzirom na to da je pod tekućim pitanjima na 139. sjednici VM-a kao tačka dnevnog reda ovaj Prijedlog pravilnika. Također, navode da u prilogu dostavljaju objedinjeni Prijedlog pravilnika u koji su sublimirali pored Jedinice interne revizije, izmijenjene strukture organizacione jedinice i naziva Sektora za azil, Sektora za informatiku i telekomunikacione sisteme.
23. 5. 2018. godine MS prema MFT-u	Predmet: Pravilnik o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, mišljenje, dostavlja se: Dostavljaju na mišljenje sa izvršenom fiskalnom procjenom uticaja za spomenuti pravilnik.
20. 7. 2018. godine MS prema MFT-u	Predmet: Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, mišljenje, traži se – urgencija: Urgencija veza na akt od 23. 5. 2018. godine na koji MFT još uvijek nije odgovorio, ni dva mjeseca nakon prvobitnog akta.
23. 8. 2018. godine MS prema MFT-u	Predmet: Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, mišljenje, traži se – urgencija: Urgencija veza na akt od 23. 5. 2018. i 20. 7. 2018. godine na koje MFT nakon čak tri mjeseca nije odgovorio. U ovoj urgenciji se MS poziva na obaveze uspostave centralne kontakt tačke i uspostave Odsjeka za saradnju sa Europolom, zatim na obavezu uspostave CERT-a.
30. 8. 2018. godine (zaprimljeno u MS 28. 11. 2018. godine) MFT prema MS-u	Predmet: Mišljenje na Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a: Između ostalog, nije usklađeno finansijski, budući da finansijska usklađenost podrazumijeva osiguranost sredstava u Budžetu institucija BiH (predloženo povećanje za 710.000 KM). MFT je mišljenja da je razvrstavanje radnog mjesta referent specijalista za prijenos tajnih podataka izvršeno suprotno odredbama Metodologije. MFT ne može podržati predloženu izmjenu, nego upućuje MS da razmotri da važeće nepopunjene pozicije zamijeni pozicijama radi kojih se dopunjava važeći pravilnik.
12. 9. 2018. godine MS prema GS-u	Predmet: Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, dostavlja se: MS u skladu s obavezama iz Sporazuma o saradnji s Europolom predlaže uspostavu Odsjeka za saradnju sa Europolom. Komisija Ministarstva pravde je dala pozitivno mišljenje na opis poslova službeničkih radnih mjesta sistematizovanih u Odsjeku za saradnju s Europolom. Za sistematizaciju Odsjeka za CERT i sigurnosti IKT sistema dato je pozitivno mišljenje Ureda za zakonodavstvo i Ministarstva pravde. Uspostavlja se i Jedinica interne revizije u skladu sa Zakonom o internoj reviziji institucija BiH za šta je dato pozitivno mišljenje MFT-a, Ureda za zakonodavstvo i Komisije

	Ministarstva pravde za analizu opisa poslova radnih mjesta državnih službenika. U Sektoru za azil, Odsjeku za prihvat i program, neophodno je povećanje broja izvršilaca. Neophodno je formirati Odsjek za centralni registar. Mišljenje MFT-a nije dostavljeno za ovu izmjenu. Na Pravilnik koji obuhvata sve izmjene i dopune koje su prethodno rađene u fazama zatraženo je mišljenje svih nadležnih institucija. Opisi poslova službeničkih radnih mjesta usklađeni su sa mišljenjem Komisije Ministarstva pravde koja je nadležna za analizu opisa poslova radnih mjesta državnih službenika, izuzev tri radna mjesta sistematizovana u Odsjeku za centralni registar, Sektora za zaštitu tajnih podataka. Mišljenje MFT-a nije dostavljeno, iako je zatraženo 23. 5. 2018. godine, te urgirano 20. 7. 2018. i 23. 8. 2018. godine. Mišljenje Ureda za zakonodavstvo od 26. 6. 2018. godine je uvaženo i ugrađeno, osim razvrstavanja ovih radnih mjesta u odgovarajuće odsjeke.
19. 9. 2018. godine GS prema MS-u	Predmet: Dopuna materijala, traži se: Nedostaje mišljenje MFT-a sa obrascem 2a o fiskalnoj procjeni uticaja. Napomena da po potrebi pribave inovirana mišljenja nadležnih institucija u slučajevima kada je pozitivnost prethodnih mišljenja bila uslovljena ugradnjom određenih sugestija.
24. 9. 2018. godine MS prema GS-u	Predmet: Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, odgovor, dostavlja se: Posebno se ističe da je u smislu realizacije Sporazuma o saradnji između Europola i BiH obaveza MS-a da najkasnije do 30. 9. 2018. godine uspostavi Odsjek za saradnju sa Europolom. Istakli su da je izostala saradnja Ministarstva pravde (na traženo mišljenje i dvije urgencije, tri mjeseca poslije im odgovorili da ne mogu dati mišljenje dok se ne dovrši postupak razvrstavanja službeničkih radnih mjesta) i saradnja sa MFT-om (na traženo mišljenje i dvije urgencije do ovog datuma nije stigao odgovor).
25. 12. 2018. godine MS prema MFT-u	Predmet: Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, mišljenje, traži se: U skladu s mišljenjem MFT-a od 30. 8. 2018. godine (koji je MS zaprimio 28. 11. 2018.) MS prihvata primjedbe i sugestije date na razvrstavanje zaposleničkih radnih mjesta u platne razrede, kao i konstataciju da je potrebno za svako zaposleničko radno mjesto precizirati kategoriju. Uz Prijedlog pravilnika je dostavljen i Obrazac 2a o fiskalnoj procjeni učinka.
21. 01. 2019. godine MS prema MFT-u	Predmet: Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a, dopuna, traži se: U prilogu akta je dostavljen Obrazac 2a o fiskalnoj procjeni učinka kao i obrazac za razvrstavanje radnih mjesta srednje stručne spreme u platne razrede C3, C4, C5.
29. 1. 2019. godine MFT prema MS-u	Predmet: Mišljenje na Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a: MFT je mišljenja da je razvrstavanje radnog mjesta referent specijalista za prijenos tajnih podataka izvršeno suprotno odredbama Metodologije. MFT sugeriše da se za svako zaposleničko radno mjesto precizira kategorija i da se ista uskladi sa platnim razredom za koju je dobijena saglasnost. Potrebno je ograničiti radne zadatke i odgovornost Odsjeka za CERT samo na informacione sisteme MS-a. U dijelu Pravilnika koji se odnosi na Odsjek za saradnju s Europolom, isti nije usklađen sa Zakonom o Direkciji za koordinaciju policijskih tijela. MFT podržava finansijski aspekt prijedloga pravilnika u dijelu koji se odnosi na sistematizovanje pozicija JIR i u Sektoru za azil, ali istovremeno upućuje predlagaoca da umjesto predloženog broja izvršilaca i sistematizovanja tri odsjeka

	razmotri sistematizovanje drugih unutrašnjih organizacionih jedinica sa manjim brojem izvršilaca.
11. 11. 2019. godine MS prema GS-u	Predmet: Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS, dostavlja se: U prilogu akta su obligatorna mišljenja nadležnih institucija. U skladu sa mišljenjima nadležnih institucija iz ovog prijedloga izostavljene su izmjene i dopune kojima bi se uspostavio Odsjek za saradnju s Europolom i Odsjek za centralni registar, tako da ovaj Pravilnik o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji obuhvata: uspostavu Jedinice interne revizije, izmjene u Sektoru za azil u smislu povećanja broja izvršilaca i uspostavu Odsjeka za CERT i sigurnost IKT sistema.
15. 11. 2019. godine GS prema MS-u	Predmet: Upit, dostavlja se: Uvidom u evidencije GS-a konstatuje da već imaju zaprimljen Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS od 12. 9. 2018. godine. S tim u vezi potrebno je da se MS hitno izjasni da li prethodno dostavljeni Prijedlog navedenog pravilnika povlači iz procedure razmatranja na sjednicama VM-a kako bi bilo jasno i nedvosmisleno koji od predloženih materijala bi članovi VM-a trebali razmotriti i o istom se izjašnjavati na sjednici.
30. 12. 2019. godine GS prema MS-u	Predmet: Pregled materijala, dostavlja se: Pregled materijala zaključno sa 26. 12. 2019. godine, na kojem je između ostalog i Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS (stari prijedlog).
06. 01. 2020. godine Kabinet ministra svim sektorima MS i upravnim organizacijama u sastavu MS-a	Predmet: Pregled materijala i zahtjev za mišljenjem, traži se: Zahtjev za kratkim obrazloženjem vezano za materijal koji će se naći na sjednici VM-a. Od sektora i ostalih se, između ostalog, traži da obrazlože razloge zbog kojih neka od navedenih tačaka treba ostati u proceduri ili ju je potrebno vratiti radi dorade.
08. 01. 2020. godine Kabinetu ministra MS-a	Predmet: Pregled materijala i zahtjeva za mišljenjem, dostavlja se: Pomoćnik ministra u Sektoru za informatiku i telekomunikacione sisteme upućuje Kabinetu ministra da je, između ostalog, Prijedlog pravilnika o unutrašnjoj organizaciji potrebno razmotriti po hitnom postupku.
08. 01. 2020. godine Kabinet ministra MS prema GS-u	Pregled: Obavijest o aktima koji su u prethodnom periodu dostavljeni u GS, dostavlja se: Obavijest za GS da iz dalje procedure, radi ažuriranja i dopune, povlače, između ostalog, i Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji MS-a (zaprimljen 15. 11. 2018. godine).
08. 10. 2020. godine Ministar sigurnosti donosi Odluku o formiranju radne skupine za pripremu Prijedloga pravilnika o unutrašnjoj organizaciji MS-a	Formira se Radna skupina za pripremu Prijedloga pravilnika o unutrašnjoj organizaciji MS-a. Radna skupina je dužna pripremiti Prijedlog pravilnika u roku od 30 dana i blagovremeno i u što kraćem roku dostaviti uz Izvještaj o urađenom u Kabinet ministra. Na sastanku stručnog kolegija MS-a, koji je održan 16. 9. 2020. godine, zatraženo je formiranje Radne grupe za pripremu Prijedloga pravilnika o unutrašnjoj organizaciji MS-a.
15. 10. 2020. godine Ministar sigurnosti donosi Odluku o izmjeni Odluke o formiranju radne skupine	Mijenja se sekretar Radne skupine. Ostali dijelovi Odluke ostaju nepromijenjeni.

26. 11. 2020. godine Radna skupina za izradu Prijedloga pravilnika o unutrašnjoj organizaciji MS-a	Zapisnik: Između ostalog, utvrđeno je da je, s obzirom na obiman materijal, pitanja koja se regulišu, usaglašavaju sa važećom zakonskom i podzakonskom regulativom, potreban duži vremenski period za pripremu Prijedloga pravilnika. Članovi Radne skupine predlažu da se prvobitno uradi procjena primjene postojeće sistematizacije, te u odnosu na rezultate, vrši i izmjena Pravilnika.
21. 01. 2021. godine Radna skupina za izradu Prijedloga pravilnika o unutrašnjoj organizaciji MS-a	Zapisnik: Između ostalog, Radna skupina se upoznala sa sadržajem prijedloga Uporedne analize važećeg Pravilnika o unutrašnjoj organizaciji sa dostavljenim materijalima ispred Sektora. Ispred svakog sektora su predložene određene izmjene, a ispred Sektora za informatiku i telekomunikacione sisteme predloženo je povećanje broja izvršilaca, koje se najviše odnosi na uspostavljanje CERT-a. Svi prisutni članovi mišljenja su da treba opravdati povećanje predloženih radnih mjesta i razmotriti mogućnost i opravdanu potrebu objedinjavanja određenih odsjeka i sektora po srodnosti poslova u skladu sa navedenim odlukama o principima i kriterijima. Na sastanku je iznesen i stav Kabineta da sistematizacija i unutrašnja organizacija treba ići u okviru važećih radnih mjesta koja su nepopunjena, a da male korekcije po pitanju radnih mjesta nisu problem.
10. 2. 2021. godine Radna skupina za izradu Prijedloga pravilnika o unutrašnjoj organizaciji MS-a	Na dnevnom redu ovog sastanka Radne skupine bila je samo jedna tačka i to razmatranje obima nadležnosti Inspektorata kao organizacione jedinice u sastavu MS-a. Nije bilo drugih tačaka dnevnog reda.
5. 3. 2021. godine Radna skupina za izradu Prijedloga pravilnika o unutrašnjoj organizaciji MS-a	Pored razmatranja informacija sa sastanka zainteresovanih sektora u pogledu obima nadležnosti Inspektorata, također je predsjedavajuća obavijestila prisutne da će opisi radnih mjesta sektora biti sastavni dio Aneksa pravilnika, te da je potrebno u što kraćem roku dostaviti obrazloženja i obrasce od strane sektora koji to do sada nisu učinili. U skladu sa diskusijom, usvojen je Zaključak: 1. Dostaviti Kabinetu ministra Prijedlog pravilnika o unutrašnjoj organizaciji, 2. Dostaviti Izvještaj sa dostavljenim obrazloženjima od strane sektora Kabinetu ministra, a koji se tiču usporedne analize važećeg Pravilnika i Prijedloga pravilnika o unutrašnjoj organizaciji, 3. Predložiti Kabinetu ministra da se formira uža Radna skupina od tri člana koja će dalje nastaviti rad na realizaciji Prijedloga pravilnika.
22. 3. 2021. godine Predsjedavajuća Radne skupine dostavlja Informaciju o rezultatima Kabinetu ministra	Radna skupina je pripremila Prijedlog pravilnika o unutrašnjoj organizaciji, osnovni tekst uz napomenu da će se Aneks pravilnika – sistematizacija radnih mjesta naknadno pripremiti u zavisnosti od konačno utvrđenog broja radnih mjesta i Izvještaj u formi usporedne analize po sektorima važećeg Pravilnika sa Prijedlogom pravilnika predloženim od strane svih sektora. Također se, između ostalog, predlaže formiranje uže Radne skupine od tri člana koja će dalje nastaviti rad na realizaciji Prijedloga pravilnika.
10. 5. 2021. godine Ministar sigurnosti donosi Odluku o formiranju Uže radne skupine koja će nastaviti rad na pripremi Prijedloga pravilnika o	Formira se uža Radna skupina koja će nastaviti dalji rad na pripremi Prijedloga pravilnika o unutrašnjoj organizaciji. Radna skupina je dužna poslove na pripremi Prijedloga pravilnika okončati blagovremeno, u što kraćem roku, dostaviti Izvještaj o urađenom u Kabinet ministra sigurnosti. Ovom Odlukom stavljaju se izvan snage Odluka o formiranju Radne skupine za pripremu Prijedloga pravilnika o unutrašnjoj organizaciji od 8. 10. 2020. godine i Odluka o izmjeni Odluke o

unutrašnjoj organizaciji MS-a	formiranju Radne skupine za pripremu Prijedloga pravilnika o unutrašnjoj organizaciji od 15. 10. 2020. godine.

Dodatak 3. Reference

1. Akcioni plan 1 uz Strategiju reforme javne uprave, 2006. godina <https://parco.gov.ba/hr/dokumenti/rju-dokumenti/akcioni-plan-1-uz-strategiju-reforme-javne-uprave/> Pristupljeno 9. 9. 2022. godine
2. Akcioni plan za period 2018 – 2022. godina, 2020. godina <https://parco.gov.ba/hr/rju/o-rju-2/strateski-okviri-za-rju/> Pristupljeno 9. 9. 2022. godine
3. Akt Evropske unije o kibersigurnosti, 2019. godina <https://eur-lex.europa.eu/legal-content/HR/LSU/?uri=CELEX:32019R0881> Pristupljeno 9. 9. 2022. godine
4. Arbanas K. "Radni okvir za procjenu i unapređenje kulture informacijske sigurnosti" Disertacija, Sveučilište u Zagrebu, Fakultet organizacije i informatike, 2021. godine
5. Bosna i Hercegovina i Europska unija, Sporazum o stabilizaciji i pridruživanju, 2008. godina <https://www.dei.gov.ba/bs/stabilization-agreement> Pristupljeno 9. 9. 2022. godine
6. Direkcija za evropske integracije, Finalni izvještaj o realizaciji akcionog plana za realizaciju prioriteta iz analitičkog izvještaja Evropske komisije, 2020. godina
7. Direktiva 2016/1148 Evropskog parlamenta i Vijeća, Direktiva o mjerama za visok zajednički nivo sigurnosti mrežnih i informacionih sistema širom Unije, 2016. godina <https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016L1148#document1> Pristupljeno 9. 9. 2022. godine
8. Evropska komisija, Izvještaj o Bosni i Hercegovini za 2021. godinu, 2021. godina <https://www.dei.gov.ba/uploads/documents/izvjestaj-o-bosni-i-hercegovini-za-2021-godinu_1636467943.pdf> Pristupljeno 9. 9. 2022. godine
9. Global Cyber Security Capacity Centre in collaboration with the World Bank, “Cybersecurity capacity review Bosnia and Herzegovina”, March 2019
10. International Telecommunication Union, “Readiness assessment report to establish a CIRT network in Bosnia and Herzegovina”, August 2018
11. ISO (2018) ISO/IEC 27000:2018(en): Information technology — Security techniques — Information security management systems — Overview and vocabulary, Velika Britanija: ISO, <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>. Pristupljeno 9. 9. 2022. godine
12. Konvencija o kibernetičkom kriminalu, Službeni glasnik Bosne i Hercegovine – Međunarodni ugovori broj: 06/06, 2006. godina
13. Ministarstvo sigurnosti Bosne i Hercegovine, „Analiza o usklađenosti pravnih propisa iz oblasti kibersigurnosti u Bosni i Hercegovini“, 2017. godina
14. Odluka o određivanju Tima za odgovor na računarske incidente za institucije Bosne i Hercegovine, Službeni glasnik Bosne i Hercegovine, broj 25/17, 2017. godina
15. Odluka o osnivanju i imenovanju ekspertne radne skupine za izvršenje svih neophodnih priprema za formiranje CERT tijela u Bosni i Hercegovini, Službeni glasnik Bosne i Hercegovine, broj 06/12, 2011. godina

16. Odluka o usvajanju Politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine za period 2017 – 2022. godine, Službeni glasnik Bosne i Hercegovine, broj 38/17, 2017. godina
17. Pravilnik o unutrašnjoj organizaciji i sistematizaciji Ministarstva sigurnosti Bosne i Hercegovine, broj: 01-02-125/09, 2009. godina
18. Program reformi Bosne i Hercegovine za period 2019 – 2020. godina, 2019. godina
19. Smjernice za strateški okvir kibersigurnosti u Bosni i Hercegovini, 2022. godina
20. Središnji državni ured za e-Hrvatsku, „Nacionalni program informacijske sigurnosti u Republici Hrvatskoj“, 2005. godina
21. Strategija i Akcijski plan kibernetičke sigurnosti Republike Hrvatske, Narodne novine 108/2015, 2015. godina
22. Strategija uspostave CERT-a u Bosni i Hercegovini, 2011. godina
23. Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, Narodne novine 68/2018, 2018. godina
24. Zakon o informacijskoj sigurnosti Republike Hrvatske, NN 79/07, 2007. godina
25. Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga Republike Hrvatske, Narodne novine 64/2018, 2018. godina
26. Zakon o kritičnim infrastrukturama Republike Hrvatske, Narodne novine 56/2013, 2013. godina
27. Zakon o ministarstvima i drugim organima uprave Bosne i Hercegovine, Službeni glasnik Bosne i Hercegovine, broj 5/03, 42/03, 26/04, 42/04, 45/06, 88/07, 35/09, 59/09, 103/09, 87/12, 6/13, 19/16 i 83/17, 2003. godina

KONTAKT

Ured za reviziju institucija Bosne i Hercegovine
Tešanjska 24a/29
71000 Sarajevo, Bosna i Hercegovina

T: + 387 33 275 400
F: + 387 33 275 401
E: saibih@revizija.gov.ba
W: www.revizija.gov.ba
@UredzaReviziju