УНИВЕРЗИТЕТ У НОВОМ САДУ
ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА
Трг Доситеја Обрадовића 6, 21000 Нови Сад, Република Србија
Деканат: 021 6350-413; 021 450-810; Централа: 021 485 2000
Рачуноводство: 021 458-220; Студентска служба: 021 6350-763
Телефакс: 021 458-133; e-mail: ftndean@uns.ac.rs
ИНТЕГРИСАНИ СИСТЕМ МЕНАЏМЕНТА СЕРТИФИКОВАН ОД:

XXIX Skup TRENDOVI RAZVOJA:

"UNIVERZITET PRED NOVIM IZAZOVIMA"

ZBORNIK RADOVA

www.trend.uns.ac.rs

2023

Uredio:

Prof. dr Boris Dumnić

Vrnjačka Banja
8 - 11. 02. 2023.

Naučno-stručni skupovi TRENDOVI RAZVOJA - TREND

1. ***skup:*** *"Informacione tehnologije i primena u elektroenergetici", Novi Sad, okt.1994.*
2. ***skup:*** *"Električna vozila – pogon i aplikacije", Novi Sad, okt. 1996.*
3. ***skup:*** *"Savremene tehnologije u elektroprivredi", Kopaonik, mart 1997.*
4. ***skup:*** *"Nove tehnologije u elektrodistribuciji", Kopaonik, mart 1998.*
5. ***skup:*** *"Nove tehnologije u elektrodistribuciji", Kopaonik, mart 1999.*
6. ***skup:*** *"Nove tehnologije u elektrodistribuciji", Kopaonik, mart 2000.*
7. ***skup:*** *"Nove tehnologije u elektrodistribuciji", Novi Sad, feb. 2001.*
8. ***skup:*** *"Univerzitet i NT parkovi", Kopaonik, feb. 2002.*
9. ***skup:*** *"Bolonjski proces I tehnički fakultetiu", Kopaonik, mart 2003.*
10. ***skup:*** *"Integrisani univerzitet i tehničke struke", Kopaonik, mart, 2004.*
11. ***skup:*** *"Šta donosi novi zakon o visokom obrazovanju", Kopaonik, mart, 2005.*
12. ***skup****: "Bolonjski proces i primena novog zakona", Kopaonik, mart, 2006.*
13. ***skup****: "Akreditacija Bolonjskih studija", Kopaonik, mart, 2007.*
14. ***skup:*** *"Efikasnost i kvalitet bolonjskih studija", Kopaonik, mart, 2008.*
15. ***skup:*** *"Doktorske studije u Srbiji, regionu i EU", Kopaonik, mart, 2009.*
16. ***skup:*** *"Bolonja 2010: stanje, dileme i perspektive", Kopaonik, mart, 2010.*
17. ***skup:*** *"EVROPA 2020: društvo zasnovano na znanju", Kopaonik, mart, 2011.*
18. ***skup:*** *"Internacionalizacija univerziteta", Kopaonik, februar, 2012.*
19. ***skup:*** *„Univerzitet na tržištu", Maribor, Slovenija, Feb. 2013.*
20. ***skup:*** *"Razvojni potencijal visokog obrazovanja", Kopaonik, Srbija, feb. 2014.*
21. ***skup:*** *"Univerzitet u promenama...", Zlatibor, Srbija, feb. 2015.*
22. ***skup:*** *"Nove tehnologije u nastavi", Zlatibor, Srbija, feb. 2016.*
23. ***skup:*** *„Položaj visokog obrazovanja i nauke u Srbiji", Zlatibor, Srbija, feb. 2017.*
24. ***skup:*** *„Digitalizacija visokog obrazovanja", Kopaonik, Srbija, feb. 2018*
25. ***skup:*** *„Kvalitet visokog obrazovanja", Kopaonik, Srbija, feb. 2019*
26. ***skup:*** *„Inovacije u modernom obrazovanju", Kopaonik, Srbija, feb.2020.*
27. ***skup:*** *„On-line nastava na univerzitetima", Novi Sad, Srbija, feb.2021.*
28. ***skup:*** *„Univerzitetsko obrazovanje za privredu", Kopaonik, Srbija, feb.2022.*
29. ***skup:*** *„On-line nastava na univerzitetima", Vrnjačka Banja, Srbija, feb.2023.*

Organizatori: **UNIVERZITET U NOVOM SADU i FAKULTET TEHNIČKIH NAUKA – NOVI SAD**

Izdavač:
Fakultet tehničkih nauka
Univerziteta u Novom Sadu
Trg Dositeja Obradovića 6, Novi Sad,
Tel: 021/ 450-810
Fax: 021/ 458-133
e-mail: ftndean@uns.ac.rs,
www.trend.uns.ac.rs

Tehnička obrada:
Havzi Sara, MSc
Nikolić Dragomir, MSc
dr Zoltan Čorba,
Nikolić Danilo, MSc

CIP - Каталогизација у публикацији
Библиотеке Матице српске, Нови Сад

378(082)

СКУП Трендови развоја (29 ; 2023 ; Врњачка Бања)
Zbornik radova [Elektronski izvor] / XXIX skup Trendovi razvoja [sa temom] "Univerzitet pred novim izazovima", Trend 2023, Vrnjačka Banja, 8-11. 02. 2023. ; uredio Boris Dumnić. - Novi Sad : Fakultet tehničkih nauka, 2023

Način pristupa (URL): http://www.trend.uns.ac.rs/stskup/trend_2023/TREND2023-ZBORNIK-RADOVA.pdf. - Opis zasnovan na stanju na dan: 22. 02. 2023.

ISBN 978-86-6022-554-4

а) Високошколско образовање -- Иновације -- Зборници

COBISS.SR-ID 108855561

Umnoženo u Novom Sadu, Februara 2023 godine.

Napomena: Organizator ne zastupa stavove, niti je odgovoran za tačnost podataka iznetih u radovima, već su to isključivo gledišta autora.

Organizaciju ovog skupa su pomogli Ministarstvo prosvete, Republike Srbije, Pokrajinski sekretarijat za visoko obrazovanje i naučnoistraživačku delatnost AP Vojvodine i IEEE Serbia and Montenegro Section-Education Society Chapter

Paper No.T2.2-2
06440

INFORMACIONA BEZBEDNOST POSMATRANA KROZ ZAKONODAVNU ZAŠTITU

Nenad Bingulac [1], Jelena Matijašević [2], Sanja Skorić [3]
[123]*Univerzitet Privredna akademija u Novom Sadu,*
Pravni fakultet za privredu i prevosuđe u Novom Sadu Srbija
[1] nbingulac@pravni-fakultet.info, [2] jelena@pravni-fakultet.info,[3] sanja@pravni-fakultet.info

Kratak sadržaj: *Kada bi se informaciona bezbednost sagledavala kroz zakonodavnu percepciju, krovni zakon kojim se uređuje ovo pitanje je Zakon o informacionoj bezbednosti. Ovim zakonom se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima. Zatim ovim zakonom se uređuju i odgovornost pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite. Primarni cilj ovog istraživanja definisan je u samom nazivu istraživanja, ali svakako u cilju preciziranja ali i svrsishodnosti načiniće se osvrt i na pojedine elemente zakona koji su od značaja za ovu temu kao što su bezbednost informaciono-komunikacioni sistem a od posebnog značaja i prevencija i zaštita od bezbednosnih rizika u informaciono-komunikacionim sistemima. Ako zakonodavnu zaštitu posmatramo kroz penalnu politiku, onda možemo da istaknemo da je zakonodavac predvideo prekršajno sankcionisanje i to isključivo novčanu kaznu, u dva različita raspona u zavisnosti od zaštitnog objekta, odnosno u zavisnosti od izvršenog prekršaja. Sekundarni cilj ovog istraživanja se odnosi na sagledavanje pitanja informacione bezbednosti iz jednog drugog ugla jer se već više pomenuta informaciona bezbednost najčešće sagledava kroz prizmu informacionih tehnologija.*

Ključne reči: informaciona bezbednost, zakonodavno predviđanje, zakonodavna zaštita, prekršajne sankcije

THE ORIGIN AND SIGNIFICANCE OF DISTANCE LEARNING AS A STANDARD IN EDUCATION

Abstract: *If information security were to be viewed through a legislative perspective, the umbrella law regulating this issue is the Law on Information Security. This law regulates protection measures against security risks in information and communication systems. Then, this law also regulates the responsibilities of legal entities when managing and using information and communication systems and determines the competent authorities for the implementation of protection measures, coordination between protection factors and monitoring of the proper application of prescribed protection measures. The primary goal of this research is defined in the name of the research itself, but certainly for the purpose of clarification but also expediency, a review will also be made of certain elements of the law that are important for this topic, such as the security of information and communication systems of special importance and prevention and protection from security risks in information and communication systems in the Republic of Serbia. If we look at legislative protection through the penal policy, then we can point out that the legislator has foreseen the sanctioning of misdemeanors, and only a fine, in two different ranges depending on the object of protection, that is, depending on the offense committed. The secondary goal of this research is related to looking at the issue of information security from a different angle, because the already mentioned information security is most often seen through the prism of information technologies.*

Key Words: information security, legislative prediction, legislative protection, misdemeanor sanctions

1. UVOD

Problematika ove teme ne može se započeti sagledavati bez (nažalost) političko bezbednostnih okolnosti i tendencija, te stoga ćemo upravo u ovom uvodnom delu rada ukazati pojedine elemente koje su naravno od isključivog značaja za temu ovog rada. Zadržaće se naravno objektivnost, bez iznošenja ličnih aspiracija.

Republika Srbija sa političko višedecenijskom tendencijom, koja predstavlja i nacionalni strateški cilj, da se postane država Evropske unije, mora da izvrši implementaciju novog zakonodavstva EU u domaće zakonodavstvo ili da izvrši usaglašavanje postojeće domaćeg zakonodavstva sa pozitivno pravnim zakonodavstvo (tj. aktuelnim) EU. U ove okolnosti, svakako, spada i zakon koji će uređivati pitanje sajber (kiber) bezbednosti, naravno, koji će biti usklađen sa politikama i principima EU. Upravo zbog iznetog, Republika Srbija donosi 2016. godine Zakon o informacionoj bezbednosti [1]

Pojedini autori koji su se više bavili pitanjem relacije Republike Srbije i NATO-a, nedvosmisleno ističu da Republika Srbija, uprkos tome što sebe prikazuje kao vojno neutralnu zemlju i koja naravno ne teži ka tome da postane članica Organizacije Severnoatlantskog ugovora (NATO), sa njom održava visok nivo saradnje. Ta saradnja se ostvaruje kroz članstvo u Partnerstvu za mir i pratećem Procesu planiranja i revizije (PARP). Pored toga, 2015. godine

Republika Srbija je dogovorila Individualni akcioni plan partnerstva (IPAP) sa NATO, uspostavljajući tako najviši nivo saradnje koje može imati zemlja koja nema aspiracije da postane članica Alijanse. Ovim sporazumom, Srbija se obavezala, između ostalog, da će preduzeti određene korake u oblasti sajber bezbednosti.[2]

Da se precizira terminologija. Termin „informaciona bezbednost" se obično koristi u kontekstu zaštite poverljivosti, integriteta i dostupnosti informacija, dok termin „sajber bezbednost" obuhvata zaštitu mreža i infrastruktura i zaštitu korisnika. U praksi, u evroatlantskom bloku zemalja termin „sajber bezbednost" se koristi u globalnim političkim debatama kao širi koncept zaštite od sajber napada, pri čemu se održava otvoren i slobodan sajber prostor, dok, na primer, zemlje Šangajske organizacije za saradnju uglavnom koriste termin „informaciona bezbednost" kao širi koncept koji dodatno uključuje pretnje u vidu informacionog rata i propagande. [3]

Organizacija za evropsku bezbednost i saradnju i UN, od Republike Srbije očekuju maksimalno zalaganje o pitanjima koja se odnose na sajber bezbednosti i da prati, primenjuje i praktikuje različite principe i mere koje promovišu i usvajaju međunarodne organizacije čiji je ona član. Iako je njihova primena dobrovoljna, merama se pružaju početne smernice, zasnovane na činjenicama i praktičnim iskustvima, za uspostavljanje i razvoj regulatornog i operativnog okvira za podizanje nacionalnog nivoa sajber bezbednosti i razvoj međunardne saradnje u toj oblasti.[2]

2. USVAJANJE ZAKONA O INFORMACIONOJ BEZBEDNOSTI

Republika Srbija (što smo već spomenuli) 2016.godine usvaja Zakon o informacionoj bezbednosti, koji je redstavlja krovni zakon kojim se regulišu mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti pravnih lica prilikom upravljanja informaciono-komunikacionim sistemima i njihovog korišćenja, te određuje nadležne organe za sprovođenje mera zaštite.

Autori koji su podrubnije analizirali ovaj novi Zakon su ukazali da jedna od najvažnijih zakonskih novina čini osnivanje Nacionalnog centra za prevenciju bezbednosnih rizika (CERT), telo zaduženo za brzo reagovanje u slučaju incidenata, kao i za prikupljanje i razmenu informacija o rizicima za bezbednost informaciono-komunikacionih sistema. Nacionalni CERT (nCERT) je u nadležnosti Regulatorne agencije za elektronske komunikacije i poštanske usluge (RATEL). Jedan od prvih koraka ovog tela je bila izrada sveobuhvatne studije izvodljivosti za osnivanje nacionalnog CERT-a, u saradnji sa Elektrotehničkim fakultetom Univerziteta u Beogradu 69 . Studija obuhvata normativnu i tehničku analizu osnivanja i funkcionisanja CERT-a u pogledu procesa i procedura, pregled komparativnih praksi u Evropi i troškova sprovođenja, akcioni plan i pregled mogućih načina finansiranja projekta međunarodnim sredstvima kojima Republika Srbija ima pristup. Takav sveobuhvatan pristup se može smatrati primerom primene principa navedenih u Zakonu o informacionoj bezbednosti, koji se odnose na upravljanje rizikom i primenu identifikovane dobre prakse. Osnivanje nacionalnog CERT-a je ujedno i jedna od osnovnih obaveza propisanih NIS Direktivom EU, pa tako i obaveza svih država članica Unije i korak koji sve zemlje kandidati treba da imaju na umu.[4]

Iz prethodnog ukazanog možemo da vidimo da za efikasno sprovođenje i funkcionisanje ovog Zakona je bilo neophodno stvaranje kohezije sa praksom.

U najkraćim crtama moramo da ukažemo na pojedine nedostake koji su postojali u Zakonu o informacionoj bezbednosti.

Po stavovima autora koji su kritikovali ovaj Zakon, najčešće se navodi da iako neupitnoj neophodnosti usvajanja zakona koji uređuje oblast informacione bezbednosti neke oblasti su ostale nedovoljno uređene, što ostavlja prostor za samostalnu interpretaciju, a može i da predstavlja potencijalni bezbednosni rizik. Zakon upućuje na princip upravljanja rizikom, ali ne propisuje eksplicitno analizu i procenu rizika ili izradu metodologije za njihovo sprovođenje, iako bi trebalo da predstavljaju osnovu za odlučivanje o adekvatnim merama zaštite, izradu i usvajanje Akta o bezbednosti IKT (skr. informaciono-komunikacioni) sistema (što je obaveza operatora) ili definisanje uloga nacionalnog CERT-a i CERT-a državnih organa, koji obezbeđuju rano upozoravanje o rizicima i ostvaruju zadatke koji se odnose na sprečavanje bezbednosnih rizika. Zakon predviđa procenu rizika samo u slučaju kompromitujućeg elektromagnetnog zračenja i samo u smislu procene rizika od neovlašćenog pristupa. U slučaju samostalnih operatora IKT sistema, bezbednosna analiza IKT sistema u smislu procene rizika pominje se samo kao mogućnost, a ne kao jasno utvrđena zakonska obaveza.[2]

Da se ne ulazi u detalje ali 2017. i 2019. godine usledile su izmene i dopune inicijalnog Zakona.

3. BEZBEDNOST IKT SISTEMA OD POSEBNOG ZNAČAJA I PREVENCIJA I ZAŠTITA OD BEZBEDNOSNIH RIZIKA U IKT SISTEMIMA

IKT sistemi od posebnog značaja su sistemi koji se koriste: 1) u obavljanju poslova u organima vlasti; 2) za obradu posebnih vrsta podataka o ličnosti, u smislu zakona koji uređuje zaštitu podataka o ličnosti; 3) u obavljanju delatnosti od opšteg interesa i drugim delatnostima i to u sledećim oblastima: (1) energetika: - proizvodnja, prenos i distribucija električne energije; - proizvodnja i prerada uglja; - istraživanje, proizvodnja, prerada, transport i distribucija nafte i promet nafte i naftnih derivata; - istraživanje, proizvodnja, prerada, transport i distribucija prirodnog i tečnog gasa; (2) saobraćaj: - železnički, poštanski, vodni i vazdušni saobraćaj; (3) zdravstvo: - zdravstvena zaštita; (4) bankarstvo i finansijska tržišta: - poslovi finansijskih institucija; - poslovi vođenja registra podataka o obavezama

fizičkih i pravnih lica prema finansijskim institucijama; - poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta; (5) digitalna infrastruktura: - razmena internet saobraćaja; - upravljanje registrom nacionalnog internet domena i sistemom za imenovanje na mreži (DNS sistemi); (6) dobra od opšteg interesa: - korišćenje, upravljanje, zaštita i unapređivanje dobara od opšteg interesa (vode, putevi, mineralne sirovine, šume, plovne reke, jezera, obale, banje, divljač, zaštićena područja);(7) usluge informacionog društva: - usluge informacionog društva) ovog zakona; (8) ostale oblasti: - elektronske komunikacije; - izdavanje službenog glasnika Republike Srbije; - upravljanje nuklearnim objektima; - proizvodnja, promet i prevoz naoružanja i vojne opreme; - upravljanje otpadom; - komunalne delatnosti; - proizvodnja i snabdevanje hemikalijama.[5]

Obaveze operatora IKT sistema od posebnog značaja su: 1) upiše IKT sistem od posebnog značaja kojim upravlja u evidenciju operatora IKT sistema od posebnog značaja; 2) preduzme mere zaštite IKT sistema od posebnog značaja; 3) donese akt o bezbednosti IKT sistema; 4) vrši proveru usklađenosti primenjenih mera zaštite IKT sistema sa aktom o bezbednosti IKT sistema i to najmanje jednom godišnje; 5) uredi odnos sa trećim licima na način koji obezbeđuje preduzimanje mera zaštite tog IKT sistema u skladu sa zakonom, ukoliko poverava aktivnosti u vezi sa IKT sistemom od posebnog značaja trećim licima; 6) dostavlja obaveštenja o incidentima koji značajno ugrožavaju informacionu bezbednost IKT sistema; 7) dostavi tačne statističke podatke o incidentima u IKT sistemu.[5]

Prevencija i zaštita od bezbednosnih rizika u ikt sistemima - Nacionalni CERT obavlja poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima u Republici Srbiji na nacionalnom nivou. Za poslove Nacionalnog CERT-a nadležna je Regulatorna agencija za elektronske komunikacije i poštanske usluge. Nacionalni CERT prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i događajima koji ugrožavaju bezbednost IKT sistema i u vezi toga obaveštava, pruža podršku, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost.[6]

Poseban centar za prevenciju bezbednosnih rizika u IKT sistemima obavlja poslove prevencije i zaštite od bezbednosnih rizika u IKT sistemima u okviru određenog pravnog lica, grupe pravnih lica, oblasti poslovanja i slično. Poseban CERT je pravno lice ili organizaciona jedinica u okviru pravnog lica sa sedištem na teritoriji Republike Srbije, koje je upisano u evidenciju posebnih CERT-ova koju vodi Nacionalni CERT. [7]

Postoji i Centar za bezbednost IKT sistema u organima vlasti koji obavlja poslove koji se odnose na zaštitu od incidenata u IKT sistemima organa vlasti, izuzev IKT sistema samostalnih operatora. Poslove CERT-a organa vlasti obavlja organ nadležan za projektovanje, razvoj, izgradnju, održavanje i unapređenje računarske mreže republičkih organa. [8]

Prethodno ukazano predviđa se aktuelnim Zakon o informacionoj bezbednosti iz 2019. godine.[9]

4. KAZNENE ODREDBE ZA KRIŠENJE PRAVNIH NORMI PREDVIĐENIH ZAKONOM O INFORMACIONOJ BEZBEDNOSTI

Zakonodavac je predvideo prekršajno sankcionisanje i to isključivo novčanu kaznu, u dva različita raspona u zavisnosti od zaštitnog objekta, odnosno u zavisnosti od izvršenog prekršaja. Prekršajne sankcije su predviđene članom 30 i 31 Zakona. [9]

Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj operator IKT sistema od posebnog značaja ako: 1) ne izvrši upis u evidenciju u roku od 90 dana od dana uspostavljanja IKT sistema od posebnog značaja 2) ne donese Akt o bezbednosti IKT sistema; 3) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema a pod tim se samtra principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti sistema, kao i ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema od posebnog značaja. 4) ne izvrši proveru usklađenosti primenjenih mera, a pod tim se podrazumeva da samostalno ili uz angažovanje spoljnih eksperata vrši proveru usklađenosti primenjenih mera IKT sistema i to najmanje jednom godišnje i da o tome sačini izveštaj. 5) ne dostavi statističke podatke a koji se odnose na incidente. Operator IKT sistema od posebnog značaja dužan je da prijavi sledeće incidente koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti: - incidente koji dovode do prekida kontinuiteta vršenja poslova i pružanja usluga, odnosno znatnih teškoća u vršenju poslova i pružanju usluga; - incidente koji utiču na veliki broj korisnika usluga, ili traju duži vremenski period; - incidente koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanja usluga, koji utiču na obavljanje poslova i vršenje usluga drugih operatora IKT sistema od posebnog značaja ili utiču na javnu bezbednost; - incidente koji dovode do prekida kontinuiteta, odnosno teškoće u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije; - incidente koji dovode do neovlašćenog pristupa zaštićenim podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose; - incidente koji su nastali kao posledica incidenta u IKT sistemu. 6) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku. Inspektor za informacionu bezbednost je ovlašćen da u postupku sprovođenja nadzora, pored nalaganja mera za koje je ovlašćen inspektor u postupku vršenja inspekcijskog nadzora utvrđenih zakonom naloži otklanjanje utvrđenih nepravilnosti i za to ostavi rok.

Do sada prikazano, u smislu kaznene politike i prekršajnih radnji je predviđeno članom 30 Zakona o informacionoj bezbednosti i odnosilo se na operatore IKT sistema, kao što smo već u ukazali na početku ovog dela, ali zakonodavac je predvideo istim članom da će se kazniti i odgovorno lice u operatoru IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj operator IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu ne obavesti predviđene organe. Operatori IKT sistema od posebnog značaja obaveštavanje o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti vrše preko veb stranice Nadležnog organa ili Nacionalnog CERT-a u jedinstveni sistem za prijem obaveštenja o incidentima kojeg održava Nadležni organ. Obaveštenje o incidentima se upućuje - Narodnoj banci Srbije, u slučaju incidenata u IKT sistemima; - regulatornom telu za elektronske komunikacije u slučaju incidenata u IKT sistemima. Zatim, u slučaju incidenata u IKT sistemima za rad sa tajnim podacima operatori tih IKT sistema postupaju u skladu sa propisima kojima se uređuje oblast zaštite tajnih podataka. 2) ne dostavlja obaveštenja o bitnim događajima u vezi sa incidentom i aktivnostima. Nakon prijave incidenta, ukoliko je incident i dalje u toku, operatori IKT sistema od posebnog značaja dostavljaju obaveštenja o bitnim događajima u vezi sa incidentom i aktivnostima koje preduzimaju do prestanka incidenta organu kome su u skladu sa ovim zakonom prijavili incident. 3) ne dostavi završni izveštaj u predviđenom roku. Operatori IKT sistema od posebnog značaja dostavljaju završni izveštaj o incidentu organu koga su u skladu sa ovim zakonom obaveštavali o incidentu u roku od 15 dana od dana prestanka incidenta, a koji obavezno sadrži vrstu i opis incidenta, vreme i trajanje incidenta, posledice koje je incident izazvao, preduzete aktivnosti radi otklanjanja posledica incidenta i, po potrebi, druge relevantne informacije.

Do sada prikazano, u smislu kaznene politike i prekršajnih radnji je predviđeno članom 31 Zakona o informacionoj bezbednosti i odnosilo se na operatore IKT sistema od posebnog značaja, kao što smo već u ukazali na početku ovog (drugog) dela, ali zakonodavac je predvideo istim članom da će se kazniti i odgovorno lice u operatoru IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

Zakonodavac je još predvideo da izuzetno od st. 1. i 2. ovog člana, ako finansijska institucija ne obavesti Narodnu banku Srbije o incidentima u IKT sistemu od posebnog značaja, Narodna banka Srbije izriče toj finansijskoj instituciji mere i kazne u skladu sa zakonom kojim se uređuje njeno poslovanje.

5. ZAKLJUČAK

U ovom radu obradili smo neke od značajnijih segmenata informacione bezbednosti ali iz jednog drugog ugla. Najčešće se ova tematika sagledava kroz prizmu informacionih tehnologija, a veoma malo, pa čak i zanemarljivo iz pravnog ugla. Cilj našeg rada je bio da se prikažu najznačajniji elementi zaštite koje predviđa zakonodavac u Zakonu o informacionoj bezbednosti, a samim tim i da prikažemo kaznene odredbe u slučaju kršenja predviđenih pravnih normi.

Smatramo da ovo predstavlja tek prvo naše istraživanje ove tematike, te stoga smo ovim radom načinili prikaz i presek postojećeg stanja, čime smo omogućili da u narednom istraživanju se dublje i preciznije posvetimo odredjenim problemima, zakonodavne prirode, za koje ćemo da probamo da predložimo adekvatne mere promene ili dopune postojeće regulative.

U ovim zaključnim razmatranjima ukazali bi još da imajući na umu kojom se brziom razvijaju aktivnosti u sajber svetu odnosno kolika je konstantna potreba za sajber bezbednošću, neophodno je prvenstveno konstantno pratiti sve evropske zakone regulativne promene, naravno i na svetskom nivou da bi se redovno ažurirali nacionalni normativni i strateški okviri. Zatim, neophodno je razvijati međudržavnu saradnju i sagledavati sve sajber trendove kako bi se u što kraćem vremenskom roku moglo zakonodavno reagovati dopunama pozitivnog zakonodavstva.

Svakako, kada je u pitanju informaciona bezbednost, ali ne pravnički-zakonodavni aspekt, apsolutno je nužno ulagati u nabavke platformi za uvežbavanje sajber napada, forenzičkih laboratorija, softvera za sajber bezbednost, nabavku hardvera i dr. Po podacima koji su nam bili dostupni, sredstva za realizaciju zakonskih obaveza ali i prethodno pomenutog, obezbeđena su od strane RATELa, kao organizacije u čijem se sastavu nalazi Nacionalni CERT.

6. LITERATURA

[1] *Zakon o informacionoj bezbednosti,* Sl. glasnik RS, br. 6/2016
[2] Aleksandar Đorđević, *Vodič kroz informacionu bezbednost u Republici Srbiji 2.0*, OEBS-a u Srbiji i Švedska agencije za međunarodnu razvojnu saradnju, Beograd, 2018.
[3] OSCE Mission, Ministerial Council Decisions on Cyber/ICT Security, www.osce.org/mission /446509
[4] Aleksandar Nešković, Natašta Nešković, *Studija izvodljivosti izgradnje nacionalnog CERT-a*, Katedra za telekomunikacije Elektrotehničkog fakulteta Univerziteta u Beogradu, 2016.
[5] Ratel, *Obaveza operatora IKT sistema od posebnog značaja*, OEBS Srbija, 2020.
[6] Ratel, *Nacionalni CERT Republike Srbije*, OEBS Srbija, 2020.
[7] Danilo Krivokapić, Andrej Petrovski, Bojan Perkov, Sonja Kolundžija, Maja Lakušić *Centar za prevenciju bezbednosnih rizika u IKT sistemima-cert,* Share Fondacija, 2019.
[8] Kancelarija za informacione tehnologije i elektronsku upravu, *Cert republičkih organa*, www.ite.gov.rs /tekst/88/cert.php
[9] *Zakon o informacionoj bezbednosti,* Sl. glasnik RS, br. 6/2016, 94/2017 i 77/2019