V E N D I M

Nr. 973, datë 02.12.2015

PËR

MIRATIMIN E DOKUMENTIT TË POLITIKAVE PËR SIGURINË KIBERNETIKE 2015 - 2017

Në mbështetje të nenit 100 të Kushtetutës, me propozimin e ministrit të Shtetit për Inovacionin dhe Administratën Publike, Këshilli i Ministrave

V E N D O S I:

1. Miratimin e dokumentit të politikave për sigurinë kibernetike 2015-2017, sipas tekstit bashkëngjitur këtij vendimi.

2. Ngarkohen ministri i Shtetit për Inovacionin dhe Administratën Publike dhe ministritë e institucionet qendrore, të përmendura në tekstin e këtij dokumenti, për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në “Fletoren zyrtare”.

Dokumenti i Politikave për Sigurinë Kibernetike 2015 - 2017

Republika e Shqipërisë

Tiranë, 2015

Pasqyra e Lëndës

Lista e Shkurtimeve

AKCE	Autoriteti Kombëtar i Certifikimit Elektronik
AKEP	Autoriteti i Komunikimeve Elektronike e Postare
AKSHI	Agjencia Kombëtare e Shoqërisë së Informacionit
ALCIRT	Agjencia Kombëtare për Sigurinë Kompjuterike
ASPA	Shkolla Shqiptare për Administratën Publike
BE	Bashkimi Evropian
DSIK	Drejtoria e Sigurimit të Informacionit të Klasifikuar
ENISA	Agjencia e Bashkimit Europian për Sigurinë e Rrjeteve dhe Informacionit (ang. European Union Agency for Network and Information Security)
FIRST	Forumi i Ekipeve të Përgjigjes ndaj Incidenteve dhe Sigurisë (ang. Forum for Incident Response and Security Teams)
ISP	Ofruesit e Shërbimit të Internetit (ang. Internet Service Provider)
IZHA	Instituti i Zhvillimit të Arsimit
IDP	Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale
ITU	Unioni Ndërkombëtar i Telekomunikacioneve
MD	Ministria e Drejtësisë
MSHIAP	Ministër Shteti për Inovacionin dhe Administratën Publike
MM	Ministria e Mbrojtjes
MPB	Ministria e Punëve të Brendshme
NATO	Organizata e Traktatit të Atlantikut Verior (ang. North Atlantic Treaty Organization)

PSH	Policia e Shtetit
SHISH	Shërbimi Informativ Shtetëror
TAIEX	Asistenca Teknike për Shkëmbimin e Informacionit (ang. Technical Assistance Information Exchange)
TF-CIRT	Task Forca e Ekipeve të Përgjigjes ndaj Incidenteve Kompjuterike (ang. Task Force Computer Incidence Response Team)
TIK	Teknologjia e Informacionit dhe Komunikimit
IMPACT	Partneriteti Shumëpalësh Ndërkombëtar Kundër Kërcënimeve Kibernetike (ang. International Multilateral Partnership Against Cyber Threats)
VKM	Vendim i Këshillit të Ministrave
CIRT	Ekipi i përgjigjes ndaj incidenteve kompjuterike (ang. Computer Incidence Response Team)
CERT	Ekipi i përgjigjes ndaj emergjencave kompjuterike (ang. Computer Emergency Response Team)
CSIRT	Ekipi i përgjigjes ndaj incidenteve të sigurisë kompjuterike (ang. Computer Security Incident Response Team)
GOVNET	Rrjeti Qeveritar (ang. Government Network)
CIIP	Mbrojtja e Infrastrukturave Kritike të Informacionit (ang. Critical Information Infrastructure Protection)

Përkufizime

Sistem kompjuterik – do të thotë çdo lloj pajisje apo grup i ndërlidhur ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi kryejnë procesime automatike të të dhënave.

Të dhëna kompjuterike - do të thotë çfarëdolloj përfaqësimi të fakteve, informacioni apo konceptesh në një formë të përshtatshme për procesim në një sistem kompjuterik, që përfshijnë një program të përshtatshëm për punën e një sistemi kompjuterik për të kryer një funksion.

Shënim*: Përkufizimet e mësipërme janë marrë nga Ligji Nr. 8888, datë 25.4.2002 "Për ratifikimin e "Konventës për krimin në fushën e kibernetikës"*

Rrjet kompjuterik - konsiderohet një rrjet telekomunikimi që i lejon kompjuterët të shkëmbejnë të dhëna.

Të dhëna personale[1] - është çdo informacion në lidhje me një person fizik, të identifikuar ose të identifikueshëm, direkt ose indirekt, në veçanti duke iu referuar një numri identifikimi ose një a më shumë faktorëve të veçantë për identitetin e tij fizik, fiziologjik, mendor, ekonomik, kulturor apo social.

Shërbim i komunikimeve elektronike[2] - është shërbimi, normalisht përkundrejt një pagese, i cili përftohet, tërësisht ose pjesërisht, nga përcjellja e sinjaleve përmes rrjeteve të komunikimeve elektronike, që përfshin shërbimet e telekomunikacioneve dhe shërbimet e transmetimit në rrjetet e përdorur për transmetime radiotelevizive dhe në rrjetet e televizionit kabllor, por duke përjashtuar shërbimet, të cilat ofrojnë përmbajtje nëpërmjet rrjeteve dhe shërbimeve të komunikimeve elektronike, ose që ushtrojnë kontroll redaksional ndaj përmbajtjes së ofruar për transmetimin, duke përdorur rrjetet dhe shërbimet e komunikimeve elektronike. Ai nuk përfshin shërbimet e shoqërisë së informacionit, të cilat nuk përbëhen, tërësisht ose pjesërisht, nga përcjellja e sinjaleve në rrjetet e komunikimeve elektronike.

Hapësirë kibernetike – konsiderohet hapësira virtuale globale e të gjithë sistemeve të informacionit dhe të komunikimit të ndërlidhur në nivel të dhënash.

Kërcënim/sulm kibernetik – konsiderohet çdo përpjekje e drejtuar/qëllimshme për të marrë

[1] LIGJ Nr. 9887, datë 10.03.2008, i ndryshuar "Për mbrojtjen e të dhënave personale"

[2] LIGJI Nr. 9918, datë 19.05.2008 për "Komunikimet elektronike në Republikën e Shqipërise**"**

akses, manipuluar, ndërhyrë ose dëmtuar integritetin, konfidencialitetin, sigurinë dhe/ose disponibilitetin e të dhënave, të një aplikimi ose të të dhënave të sistemit kompjuterik, pa patur autoritet ligjor për ta bërë këtë.

Krim kibernetik – konsiderohet ndërhyrje e paautorizuar drejt dhe/ose përmes përdorimit të TIK, penalizimi për të cilin rregullohet në Kodin Penal të Republikës së Shqipërisë.[3]

Infrastruktura kritike të informacionit – konsiderohen sistemet dhe rrjetet e informacionit dhe komunikimit, cënimi apo shkatërrimi i të cilave do të kishte impakt serioz në shëndetin, sigurinë, dhe/ose mirëqënien ekonomike të qytetarëve, dhe/ose funksionimin efektiv të ekonomisë të Republikës së Shqipërisë.

Luftë kibernetike – konsiderohet çdo akt lufte në dhe/ose përreth hapësirës kibernetike që lidhet kryesisht me teknologjinë e informacionit.

Spiunazh kibernetik – konsiderohet sulmi kibernetik që ka si objekt të tij cënimin e konfidencialitetit të një sistemi TIK (psh. spiunimi dixhital).

Sabotazh kibernetik – konsiderohet sulmi kibernetik që ka si objekt të tij cënimin e integritetit dhe disponueshmërisë së një sistemi TIK**.**

Shënim: *Në këtë Dokument vetëm për efekt standardizimi në mënyrën e të shprehurit fjala 'kompjuterike' dhe 'kibernetike' do të konsiderohen ekuivalente.*

[3] LIGJ Nr. 9859, datë 21.1.2008 "Për disa shtesa dhe ndryshime në ligjin nr.7895, datë 27.1.1995 "Kodi penal i Republikës së Shqipërisë", të ndryshuar
LIGJ Nr. 10023, datë 27.11.2008 "Për disa shtesa dhe ndryshime në ligjin nr.7895, datë 27.1.1995 "Kodi penal i Republikës së Shqipërisë", të ndryshuar
LIGJ Nr. 10054, datë 29.12.2008 "Për disa shtesa dhe ndryshime në ligjin nr.7905, datë 21.3.1995 "Kodi i procedurës penale i Republikës së Shqipërisë", të ndryshuar
LIGJ Nr. 144/2013 "Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995 "Kodi penal i Republikës së Shqipërisë", të ndryshuar

Hyrje

Me zhvillimet e shpejta të teknologjisë së informacionit dhe komunikimit, me shtrirjen e përdorimit të saj pothuajse në të gjitha fushat e veprimtarisë së shoqërisë, bëhet evidente kërkesa për shërbime të sigurta dhe të besueshme. Rritja e përdorimit të TIK dhe internetit po ndryshon shoqërinë duke krijuar mënyra të reja të lidhjes, komunikimit, bashkëpunimit dhe të zhvillimit ekonomik nëpërmjet aksesit në hapësirën kibernetike. Kjo ka bërë që shoqëria jonë të varet gjithnjë e më shumë në përdorimin e këtyre teknologjive.

> Aksesi në hapësirën kibernetike së bashku me elementët pozitivë të tij rrit rrezikun potencial nga dëmtimi apo keqpërdorimi i të dhënave dhe sistemeve kompjuterike. Si pasojë e rreziqeve kibernetike në rritje, sigurimi i integritetit të të dhënave dhe konfencialitetit si dhe një akses i sigurtë në hapësirën kibernetike, janë kthyer në një nga sfidat më të mëdha me të cilat përballet shoqëria në ditët e sotme duke e kthyer atë në një çështje të sigurisë kombëtare.

Shqipëria renditet ndër vendet ku zhvillimi i telekomunikacionit, qasja në internet dhe informatizimi i shoqërisë përparon shumë shpejt. Rritja e përdorimit të komunikimit përbën një vlerë të shtuar në zhvillimin ekonomik dhe shoqëror të vendit, por, në të njëjtën kohë, ajo e ekspozon atë ndaj rreziqeve të natyrës kibernetike me aktorë shtetërorë dhe jo shtetërorë. Sulmet kibernetike kanë potencial për të dëmtuar rëndë shkëmbimin e informacionit në institucionet publike, të telekomunikacionit dhe sistemin financiar e bankar, duke shkaktuar edhe ndërprerje të shërbimeve jetike.[4]

Ky Dokument është në mbështetje të Programit të ri të investimeve në TIK të qeverisë shqiptare:

- Përmirësimi i shërbimeve ndaj publikut;
- Një shoqëri informacioni e sigurtë; si dhe

Strategjinë e Sigurisë Kombëtare 2014-2020 (cit. '..për vendosjen dhe respektimin e standardeve më të larta në drejtim të ruajtjes dhe mbrojtjes së informacionit në të gjitha trajtat e ekzistencës së tij, duke përqendruar përpjekje të veçanta për mbrojtjen nga sulmet kibernetike').

[4] Strategjia e Sigurisë Kombëtare (SSK), 2014 – 2020

Ky Dokument është gjithashtu në linjë me Agjendën Dixhitale për Evropën 2020 (cit. Rritja e besimit në TIK nëpërmjet forcimit të politikës së sigurisë për rrjetet dhe informacionin) si dhe në linjë me Strategjinë për Sigurinë Kibernetike të Bashkimit Evropian: Hapësirë kibernetike e hapur, e sigurt dhe e mbrojtur (ang. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace).

Qëllimi i këtij Dokumenti Politikash është të rishikojë dhe të koordinojë detyrimet që lindin nga angazhimet e marra për një hapësirë kibernetike të sigurt me qëllim që të sigurohet përmbushja e përgjegjësive nga të gjithë aktorët në mënyrë të koordinuar. Në këtë mënyrë mund të garantohet zhvillimi i mëtejshëm i shoqërisë së informacionit si një ambient i sigurt, i besueshëm dhe i hapur si dhe promovimin e vlerave dhe mundësive të ofruara nga përdorimi i hapësirës kibernetike.

Dokumenti pas nje analize të situatës dhe zhvillimeve aktuale, përcakton vizionin dhe objektivat e zhvillimit për periudhën 2015-2017 si dhe jep drejtimet kryesore të politikave që do të ndiqen për realizimin e këtyre objektivave. Dokumenti mbështetet në modelet dhe praktikat më të mira evropiane, përsa i përket objektivave dhe zgjidhjeve të parashikuara, gjithnjë duke marrë në konsideratë karakteristikat specifike të shoqërisë dhe ekonomisë shqiptare.

Ky Dokument Politikash është i shoqëruar dhe me një plan veprimi, i cili do të jetë objekt rishikimi të paktën një herë në vit. Dokumentet kryesore ku është mbështetur Dokumenti i Politikave për Sigurinë Kibernetike 2015 - 2017 janë:

- Axhenda Dixhitale e Shqipërisë (2014 - 2020)
- Strategjia e Sigurisë Kombëtare (SSK)
- Strategjia për Sigurinë Kibernetike e Bashkimit Europian: Hapësirë kibernetike e hapur, e sigurt dhe e mbrojtur (ang. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace)[5]

Në hartimin e këtij dokumenti kanë marrë pjesë të gjitha palët e interesit nga sektori publik dhe privat, si dhe është ndihmuar nga ekspertët e Bashkimit Evropian përmes misionit të TAIEX-it.

[5] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - Join(2013) 1 final - 7/2/2013

Situata aktuale në Shqipëri

Strategjia Ndërsektoriale për Shoqërinë e Informacionit 2008-2013 (SNSHI) e miratuar me VKM Nr. 59 dt. 21.1.2009 përveçse përbën dokumentin strategjik që përcaktonte drejtimet kryesore dhe objektivat e zhvillimit në fushën e shoqërisë së informacionit për periudhën 2008 – 2013 ishte edhe dokumenti i vetëm ku përmendej shkurtimisht siguria kibernetike si një nga fushat që duhej konsideruar me prioritet për shkak të vizionit të Qeverisë shqiptare për të rritur e zhvilluar e-qeverisjen përmes ofrimit të e-shërbimeve.
Siguria kompjuterike përmendej në Iniciativat në Fushën e Shoqërisë së Informacionit në SNSHI si më poshtë:

- Siguria e fëmijëve online dhe nxitja e koordinimi i procesit për kodet e sjelljes
- Krijimi i Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT)
- Krijimi i infrastrukturës PKI dhe ofrimi i shërbimeve të sigurta

Në mbështetje me Ligjin "Për mbrojtjen e të drejtave të fëmijëve", "Planin e Veprimit për fëmijë 2012 -2015" miratuar me Vendim të Këshillit të Ministrave nr. 182 datë 13.03.2012, legjislacionin shqiptar në fuqi dhe praktikën më të mirë evropiane në këtë drejtim; "Parimet për Rrjete Sociale më të Sigurta për vendet e BE-së", të Komisionit Evropian publikuar në Shkurt të vitit 2009 si dhe dokumentin "Kuadri Evropian për një përdorim më të sigurt të Celularit nga Adoleshentët dhe Fëmijët", nënshkruar nga operatorë të ndryshëm në Evropë, në Shkurt të vitit 2007; më 7 Shkurt 2013 u nënshkrua nga operatorë shqiptarë “Kodi i sjelljes për përdorimin e sigurtë dhe të përgjegjshëm të rrjeteve dhe të shërbimeve të komunikimeve elektronike në Shqipëri”.

Gjithashtu në zbatim të Strategjisë Ndërsektoriale për Shoqërinë e Informacionit 2008-2013 (SNSHI), Agjencia Kombëtare e Shoqërisë së Informacionit ka ofruar:

- Autentifikim dhe identifikim të sigurtë – për 25 institucione, 2500 përdorues;
- Internet të sigurtë për 65 institucione;
- Instalim automatik dhe qendror të aplikimeve – 2000 PC të Ministrive që janë në domain;
- Menaxhim qendror i mbrojtjes antivirus – 7 institucione, 1000 kompjutera;
- E-signature përmes Infrastrukturës Qeveritare të Çelësit Publik (PKI) – 2 institucione;

Përdorimi i Teknologjisë së Informacionit dhe Komunikimit është rritur ndjeshëm në vitet e fundit.

Sipas të dhënave të publikuara nga AKEP, numri i përdoruesve aktivë të shërbimeve celulare në fund të vitit 2013 ishte afërsisht 3.7 milion përdorues. Penetrimi i telefonisë celulare bazuar në kartat SIM aktive arriti në 130%.

Aksesi broadband Internet ka pasur rritje të ndjeshme si për lidhjet broadband fiks me 14% gjatë vitit 2013, ashtu dhe në mobile broadband, respektivisht për lidhjet me kartë modem dhe USB me 88 - 101% gjatë vitit 2013. Në total numri i pajtimtarëve broadband (fiks e mobile) është rritur me 36% gjatë vitit 2013.

Numri total i lidhjeve broadband fiks në fund të vitit 2013 arriti në 182.556 dhe përdorues të shërbimeve broadband bazuar në celular arriti në fund të vitit 2013 në 1.231.269.

Përdoruesit e Internetit në Shqipëri janë rritur me disa herë në vitet e fundit. Sipas të dhënave të publikuara nga Bashkimi Ndërkombëtar i Telekomunikacionit, penetrimi i Internetit në Shqipëri në dhjetë vitet e fundit është rritur nga 0.97% në vitin 2003 në mbi 60% në vitin 2013.[6]

Viti	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**
Shqipëria	0.97	2.42	6.04	9.61	15.04	23.86	41.20	45.00	49.00	54.66	60.10

Ndërkohë që numri i shkeljeve të sigurisë së rrjeteve dhe sigurisë së informacionit është duke u rritur me shpejtësi. Kjo shkakton humbje financiare dhe krijon rreziqe dhe kërcënime të reja për zhvillimin e Shoqërisë së Informacionit. Në këtë kuadër është e domosdoshme që të ndërmerren hapa për zhvillim të sigurt të Shoqërisë së Informacionit.

Nga të dhënat zyrtare të Policisë së Shtetit mbi krimin kibernetik, të rregulluar sipas Kodit Penal të Republikës së Shqipërisë, rezultojnë se në periudhën Janar - Dhjetor 2014 janë evidentuar **180** vepra penale, janë zbuluar **76**, me **86** autorë, nga të cilët **74** janë në gjëndje të lirë, **10** të arrestuar dhe **2** në kërkim. Për periudhën Janar – Dhjetor 2013, janë evidentuar **108** vepra penale nga të cilat janë zbuluar **63** prej tyre, me **69** autorë, nga të cilët **58** janë në gjëndje të lirë, **9** arrestuar dhe **2** në kërkim.

[6] Burimi: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Krahasuar me të njëjtën periudhë të vitit të kaluar, janë evidentuar **66%** më shumë vepra penale, me **17** autorë më shumë, **1** autor të arrestuar më shumë.

Të ndara sipas veprave penale ato paraqiten si më poshtë:

- Neni 119/a, "Shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik", evidentuar **1** rast, pa autor;
- Neni 143/b, "Mashtrimi Kompjuterik", evidentuar **49** raste, me **14** autorë në gjëndje të lirë, **1** i arrestuar;
- Neni 186/a, "Falsifikim Kompjuterik'', evidentuar **28** raste, me **20** autor, nga të cilët **4** arrestuar dhe **16** në gjëndje të lirë;
- Neni 192/b, "Hyrja e paautorizuar kompjuterike", evidentuar **14** raste, me **7** autorë në gjendje të lirë;
- Neni 293/a, "Përgjimi i paligjshëm i të dhënave kompjuterike", evidentuar **1** rast me **2** autorë, në gjendje të lirë;
- Neni 293/b, "Ndërhyrja në të dhënat kompjuterike", evidentuar **33** raste me **16** autorë, nga të cilët **2** të arrestuar dhe **14** në gjëndje të lirë;
- Neni 293/c, "Ndërhyrja në sistemet kompjuterike", evidentuar **4** raste, me **3** autorë në gjendje të lirë;
- Neni 121 "Ndërhyrje të padrejta në jetën private", **4** raste, pa autor;
- Neni 117, paragrafi i tretë, "Pornografia", evidentuar **38** raste me **14** autorë në gjendje të lirë;
- Neni 121/a "Përndjekja", evidentuar **4** vepër penale, zbuluar **3**, me **2** autorë të proceduar në gjëndje të lirë, **1** i arrestuar;
- Neni 137/a "Vjedhja e rrjetit të komunikimeve elektronike", evidentuar **1** vepër penale, zbuluar **1**, me **1** autor në gjëndje të lirë;
- Neni 149/a "Shkelja e të drejtave të pronësisë industriale", evidentuar **1** vepër penale, zbuluar **1**, me **1** autor i cili është proceduar në gjendje të lirë.
- Shpifja e parashikuar nga neni 120 i Kodit Penal, evidentuar **1** rast me **1** autor në gjendje të lirë.

Këto vepra penale të ndara sipas drejtimeve:

Nr	Krime Kompjuterike	Evidentuar	Zbuluar	Autorë gjithsej	Arrestuar	Gjendje të lirë	Larguar
1	Në fushën e teknologjisë dhe informacionit	53	29	30	2	28	-
2	Nëpërmjet sistemit kompjuterik	127	47	56	8	50	-
3	**Gjithsej**	**180**	**76**	**86**	**10**	**78**	**-**

Sipas Drejtorive të Policisë së Qarqeve, veprat penale të evidentuara ndahen si më poshtë:

Nr	Drejtoria e Policisë së Qarkut	VP të evidentuara	VP të zbuluara	Autorë Gjithsej	Arrestuar e ndaluar	Në gjendje të lirë
1	Durrës	7	1	1		1
2	Korca	4	2	2		2
3	Dibër	1	-	-	-	-
4	Berat	1	-	-	-	-
5	Fier	5	4	4	-	4
6	Elbasan	5	4	4		4
7	Shkodër	9	3	3	-	3
8	Kukës	2	2	3	3	-
9	Lezhë	3	3	3	-	3
10	Tiranë	61	27	31	6	25
11	Vlorë	6	4	5	-	5
12	Qendra	77	27	30	1	29
	Shuma krime kompjuterike	**181**	**77**	**86**	**10**	**76**

Rëndësi të veçantë merr iniciimi i ndryshimeve ligjore në mënyrë që të ofrohet mbrojtje e përshtatshme për përdoruesit, për të rritur besimin e tyre në teknologjitë e informacionit dhe për të inkurajuar përdorimin e avancuar dhe të sigurt të TIK-ut.

Vlerësohet si tejet e nevojshme marrja e veprimeve dhe masave specifike për të ndërgjegjësuar shoqërinë lidhur me rreziqet potenciale në fushën e sigurisë së rrjeteve dhe sistemeve për eliminimin e këtyre rreziqeve, përfshirë mbrojtjen e fëmijëve nga përmbajtjet e paligjshme në hapësirën kibernetike.

Sulmet në infrastrukturat kritike të informacionit në rang vendi mund të kenë pasoja të rënda në funksionalitetin e tyre duke shkaktuar edhe humbje të mëdha financiare, prandaj lind nevoja që së pari ato të identifikohen e më pas të merren masa të forta sigurie për ta mbajtur në nivel më të lartë sigurinë e këtyre infrastrukturave si më jetike për funksionimin e shoqërisë. [7]

[7] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - Join(2013) 1 final - 7/2/2013

Kuadri ligjor dhe institucional

Zhvillimi i shpejtë i TIK kushtëzohet dhe nga përshtatja e legjislacionit përkatës të nevojshëm. Në përgjithësi Shqipëria është në pajtueshmëri me detyrimet që rrjedhin nga MSA-ja në këtë fushë. Ka disa ligje që rregullojnë ndjekjen penale të krimeve kompjuterike në Republikën e Shqipërisë si: Ligji Nr. 8888 i datës 25.04.2002 "Për Ratifikimin e Konventës për Krimin Kibernetik" është reflektuar në Kodin Penal si dhe Ligji Nr. 9262 i datës 29.07.2004 "Për Ratifikimin e Protokollit shtesë të Konventës për krimin kibernetik, për penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike" sërish është reflektuar në Kodin Penal përkatësisht në Ligjin Nr. 9859, datë 21.1.2008 "Për disa Shtesa dhe Ndryshime në Ligjin Nr.7895, datë 27.1.1995", "Kodi Penal i R.Sh" dhe Ligji Nr. 10023, datë 27.11.2008 për disa Shtesa dhe ndryshime në Ligjin Nr. 7895, datë 27.1.1995 "Kodi Penal i Republikës Së Shqipërisë; dhe Ligji Nr. 10054, datë 29.12.2008 Për disa shtesa dhe ndryshime në Ligjin Nr. 7905, datë 21.3.1995.[8]

Kuadri ligjor i strukturave qeveritare që merren me sigurinë dhe krimin kibernetik në Shqipëri

Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT), është autoriteti qendror për identifikimin, parashikimin dhe marrjen e masave për mbrojtjen ndaj kërcënimeve/sulmeve kompjuterike, në përputhje me legjislacionin në fuqi.

Drejtoria e Sigurimit të Informacionit të Klasifikuar (DSIK), është autoriteti që kontrollon, garanton sigurinë e sistemeve të klasifikuara të komunikimit dhe informacionit dhe bën akreditimin e tyre nëpërmjet lëshimit të Çertifikatës së Sigurisë për këto të fundit.

Autoriteti Kombëtar për Certifikimin Elektronik (AKCE), është autoriteti që ka përgjegjësinë e mbikëqyrjes së zbatimit të Ligjit "Për Nënshkrimin Elektronik" dhe të akteve nënligjore të nxjerra në zbatim të tij. AKCE bën akreditimin e ofruesve të shërbimit të certifikimit elektronik.

[8] Per ndryshime te metejshme ne Kodin Penal, referoju Ligjit nr. 144/2013 "Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", të ndryshuar

Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI), është përgjegjëse për administrimin e infrastrukturës qeveritare të Çelësit Publik (PKI) dhe siguron pajtueshmërinë me nenin 19 të ligjit nr.9880, datë 25.2.2008 "Për nënshkrimin elektronik". Në shërbimet që ofron në Qendrën e të Dhënave Qeveritare, për administratën publike, garanton autentifikim dhe identifikim të sigurtë, internet të sigurtë dhe DNS të sigurtë.

Policia e Shtetit, është organi përgjegjës për parandalimin, zbulimin dhe hetimin e veprave penale, ndër të cilat përfshihen dhe veprat penale në fushën e TIK, që ndiqen nga Sektori i Kundër Krimit Kompjuterik.

Prokuroria e Përgjithshme, përmes sektorit të krimeve kibernetike ushtron ndjekjen penale për vepra penale në fushën e kibernetikës. Kjo strukturë kontrollon aktivitetin e njësive të posaçme për ndjekjen e krimeve kibernetike, që janë ngritur në prokuroritë e rretheve gjyqësore.

Shërbimi Informativ i Shtetit (SHISH), përmes seksionit të Kundër Krimit Kibernetik, ka për detyrë kërkimin, zbulimin dhe analizimin e krimeve kibernetike që cënojnë sigurinë kombëtare.[9]

Ministria e Mbrojtjes, ka rol në ruajtjen e sigurisë kibernetike përmes Drejtorisë së Automatizimit dhe Inovacionit, por edhe institucioneve të përmendura më poshtë në varësi të Ministrit të Mbrojtjes (DSH dhe AISM).

Shtabi i Përgjithshëm i Forcave të Armatosura të Republikës së Shqipërisë, Drejtoria e Ndërlidhjes, përgjigjet për zhvillimin e Sistemeve të ndërlidhjes dhe të Informacionit (SNI) në Forcat e Armatosura të Republikës së Shqipërisë duke u mbështetur në standardet kombëtare, të NATO-s dhe ato ndërkombëtare.

Drejtoria e Shifrës (DSH), është Autoriteti Kombëtar për Sigurimin e Komunikimeve dhe Autoritet Kombëtar i Shpërndarjes.[9]

Agjencia e Inteligjencës së Mbrojtjes dhe Sigurisë (AISM), përmes sektorit të Mbrojtjes Kibernetike dhe Infosec ka si detyrë parashikimin, identifikimin dhe analizimin e kërcënimeve kibernetike që cënojnë sistemet TIK të FASH.

[9] LIGJ Nr.8457, date 11.2.1999 "Për informacionin e klasifikuar "Sekret Shtetëror"
VKM Nr. 922 datë 19.12.2007 "Për sigurimin e informacionit të klasifikuar "Sekret Shtetëror" që prodhohet, ruhet, përpunohet apo transmetohet në sistemet e komunikimit (INFOSEC)"
VKM Nr.690, datë 5.10.2011 "Për miratimin e rregullores "Për mbrojtjen kriptografike të informacionit të klasifikuar "Sekret Shtetëror""

Banka e Shqipërisë (BSH), ka autoritetin e organit që ka të drejtën ekskluzive të japë miratimin për fillimin e aktivitetit bankar nëpërmjet dhënies së licencës, si dhe të mbikqyrë aktivitetin e çdo subjekti, i cili ka marrë licencë për ushtrimin e veprimtarisë bankare në Republikën e Shqipërisë. Në fushën e sigurisë së sistemeve të tij TIK, subjekti përcakton objektiva, strategji dhe kërkesa të sigurisë si dhe miraton procedura për administrimin, për operimin, për ruajtjen e sistemeve, për mbrojtjen e të dhënave si edhe për nxjerrjen jashtë përdorimit te tyre.

Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP), mbikëqyr, kontrollon dhe monitoron veprimtaritë e sipërmarrësve të rrjeteve të komunikimeve elektronike dhe të shërbimeve të komunikimeve të elektronike. AKEP-i, mbikëqyr zbatimin e masave të nevojshme të ndërmarra nga sipërmarrësit mbi sigurinë dhe integritetin e shërbimeve dhe rrjeteve të komunikimeve elektronike publike në lidhje me mbrojtjen e të dhënave personale.

Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (IDP), është autoriteti përgjegjës i pavarur, që mbikqyr dhe monitoron, në përputhje me ligjin, mbrojtjen e të dhënave personale elektronike gjatë ruajtes, përpunimit dhe transmetimit të tyre, duke respektuar e garantuar të drejtat dhe liritë themelore të njeriut.

Institucione të tjera mbështetëse në arritjen e objektivave të Dokumentit

Shkolla Shqiptare e Administratës Publike (ASPA), është organi që ka si detyrë formimin, trajnimin profesional të nëpunësve të administratës të cilat fokusohen në ngritjen e kapaciteteve menaxhuese të qëndrueshme; rritjen e përgjegjshmërisë së punonjësve të administratës; krijimin e një trupe funksionarësh publikë profesionistë, të paanshëm dhe eficentë në kryerjen e funksioneve të tyre. Ky institucion do të ofrojë ndihmë për organizimin e trajnimeve për profesionistët IT të administratës publike.

Instituti i Zhvillimit të Arsimit (IZHA), është institucioni që ka si detyrë hartimin e kurrikulës së TIK-ut për arsimin parauniversitar (k-12), e cila përmban tematika shumë të rëndësishme, të fushës së sigurisë kibernetike, përmbajtja e të cilave konsiston në përdorimin e sigurtë të internetit nga nxënësit dhe mësuesit.

Në bazë të VKM Nr. 303, datë 31.3.2011 "Për krijimin e njësive të teknologjisë së informacionit e të komunikimit në ministritë e linjës dhe institucionet e varësisë" çdo institucion ka Drejtori TI, e

cila është përgjegjëse për sigurinë në sistemet e TIK dhe në këtë kuadër ka edhe përgjegjësi për sigurinë kibernetike.

Vizioni, parimet dhe objektivat strategjike

KY DOKUMENT PËRCAKTON SI VIZION:

Për një hapësirë kibernetike më të sigurtë, më të besueshme dhe më të qëndrueshme për qytetarët, biznesin dhe qeverinë në mbështetje të zhvillimit ekonomik dhe social të Shqipërisë.

Hapësira kibernetike duhet parë si një fushë shumë dimensionale, me shumë shtresa dhe gjerësi territoriale përtej kufijve kombëtarë. Realizimi i një sigurie kibernetike duhet të mbështetet në këto parime bazë:

- **Mbrojtja e të drejtave themelore të njeriut, lirinë e shprehjes, të dhënat personale dhe privatësinë:** Siguria kibernetike mund të jetë efikase vetëm nëse ajo është e bazuar në të drejtat dhe liritë themelore të njeriut sipas Kartës së të Drejtave Themelore të Bashkimit Evropian dhe vlerave thelbësore të BE. Reciprokisht, të drejtat e individëve nuk mund të sigurohen pa rrjete dhe sisteme të sigurta. Çdo shkëmbim informacioni, kur përfshin të dhënat personale, duhet të jetë në përputhje me ligjin e mbrojtjes së të dhënave të BE-së si dhe Ligjin Nr. 9887, datë 10.03.2008, i ndryshuar "Për mbrojtjen e të dhënave personale" dhe të marrë parasysh të drejtat e individëve në këtë fushë.

- **Akses për të gjithë:** Aksesi i kufizuar dhe/ose pamundësia për akses në internet si dhe analfabetizmi dixhital përbëjnë një disavantazh për qytetarët, duke pasur parasysh sesa bota dixhitale përshkon veprimtarinë brenda shoqërisë. Çdo njeri duhet të jetë në gjendje të aksesojë internetin dhe të ketë rrjedhë të pakufizuar informacioni. Integriteti dhe siguria e internetit duhet të jenë të garantuara për të lejuar akses të sigurt për të gjithë.

- **Përgjegjësi e përbashkët**: Siguria kibernetike nuk mund të konsiderohet si një problem i cili prek apo i takon një institucioni, institucioneve shtetërore, sektorit privat ose qytetarëve. Ajo është problem i cili prek gjithë fushat e jetës dhe shoqërisë. Si i tillë kërkon

marrjen e masave të nevojshme të sigurisë nga të gjithë përdoruesit e teknologjisë TIK dhe hapësirës kibernetike.

- **Forcimi i bashkëpunimit dhe koordinimit**: Bazuar në përgjegjësitë e përbashkëta është e nevojshme rritja e bashkëpunimit dhe e koordinimit mes të gjithë aktorëve. Forcimi i bashkëpunimit ndërinstitucional, bashkëpunimi me sektorin privat dhe publik, bashkëpunimi me botën akademike janë të domosdoshme për të arritur qëllimin.

- **Bashkëpunimi ndërkombëtar**: Hapësira kibernetike si një hapësirë pa kufij kërkon një bashkëpunim dhe koordinim ndërkombëtar për të garantuar sigurinë kibernetike. Gjithashtu me anëtarësimin në NATO dhe progresin e bërë drejt anëtarësimit në BE, Shqipëria gjithnjë e më shumë është pjesë aktive e iniciativave dhe programeve të sigurisë kibernetike dhe duhet të përmbushë angazhimet e saj ndaj vendeve aleate.

- **Administrimi i rrezikut**: Rritja e përdorimit të TIK dhe tendenca për një botë gjithnjë e më të ndërlidhur rrit dhe rreziqet me të cilat përballemi. Shqipëria do marrë masat e nevojshme për administrimin e rrezikut bazuar në standardet dhe praktikat më të mira për të garantuar sigurinë kibernetike.

- **Respektimi i vlerave**: Ky dokument do shërbejë si orientim për marrjen e të gjithë masave, hartimin e politikave, standardeve, udhëzimeve dhe procedurave për të siguruar një mbrojtje ndaj rreziqeve kibernetike duke respektuar në çdo moment parimet e të drejtave dhe lirive themelore si dhe parime të tjera demokratike.

Objektivat strategjike që do të ndiqen për përmbushjen e këtij vizioni dhe respektimin e parimeve të mësipërme janë:

i. Plotësimi i kuadrit ligjor në fushën e sigurisë kibernetike
ii. Forcimi i kuadrit institucional
iii. Rritja e ndërgjegjësimit për sigurinë kibernetike
iv. Identifikimi dhe mbrojtja e Infrastrukturave Kritike të Informacionit
v. Krijimi dhe implementimi i kërkesave minimale të sigurisë kibernetike

vi. Forcimi i partneritetit me struktura të tjera përgjegjëse të fushës brenda dhe jashtë vendit
vii. Rritja e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike.

Politikat për tu ndjekur

Plotësimi i kuadrit ligjor në fushën e sigurisë kibernetike

Në përputhje me zhvillimet dhe iniciativat do të ndërmerren hapat e nevojshëm për të analizuar, përshtatur dhe plotësuar legjislacionin në fushën kibernetike. Në mënyrë të vazhdueshme do të bëhet vlerësimi i praktikave më të mira botërore, rekomandimeve dhe iniciativave ndërkombëtare të fushës në mënyrë të veçantë ato të NATO dhe BE, duke përshtatur masat në fushën e sigurisë kibernetike në përputhje me angazhimet e marra ndaj partnerëve ndërkombëtarë. Nëse do të konsiderohet e nevojshme do të bëhet përshtatja dhe miratimi i tyre duke garantuar kështu forcimin e sigurisë kibernetike dhe luftën kundër krimit kibernetik. Në analizën e kryer në funksion të këtij Dokumenti rezulton se kuadri ekzistues ligjor dhe institucional ka disa paqartësi të cilat duhen adresuar, gjatë plotësimit të legjislacionit, si më poshtë:

a) Modernizimin e legjislacionit në fuqi dhe rishikimin periodik të tij për të adresuar sigurinë kibernetike të lidhur me zhvillimet e hapësirës kibernetike në Shqipëri dhe harmonizimin me legjislacionin ndërkombëtar, me qëllim që ai të ngelet i përshtatshëm dhe efektiv. Për të nxitur përdorimin e nënshkrimit elektronik të kualifikuar në transaksionet elektronike janë në proces këto iniciativa:
   - Hartimi i draftligjit për përdorimin e identifikimit elektronik të sigurtë, vulave elektronike në shërbimet e qeverisjes elektronike; me qëllim garantimin e identitetit në botën virtuale qoftë ky për personat fizik dhe ata juridik. Aktualisht draftligji "Për identifikimin elektronik dhe shërbimet e besuara" është në proces konsultimi në Kuvend. Ndërkohë është gati rregullorja e harmonizuar me direktivën evropiane 910/2014 për zbatimin e ligjit, e cila pritet të miratohet me vendim të Këshilit të Ministrave pas miratimit të draftligjit. Kjo paketë ligjore pritet të rrisë besimin në ambientin online me qëllim zhvillimin ekonomik dhe social, duke rritur besimin

mungesa e të cilit deri më sot ka bërë që të ketë pasiguri ligjore e cila i bën konsumatorët, bizneset dhe autoritetet publike të hezitojnë në kryerjen e transaksioneve online.

- Do të futet përdorimi sa më i gjerë i certifikatave për faqe interneti dhe web servera për të garantuar identitetin e sigurt të faqeve të institucioneve publike dhe kompanive të tjera private të cilat ofrojnë shërbime elektronike në bashkëveprim të institucioneve publike ndaj qytetarëve, apo ndaj biznesit.

b) Urdhërimi/detyrimi i kryerjes së auditimit periodik dhe vlerësimit të përshtatshmërisë dhe efektivitetit të sigurisë së sistemeve të informacionit në përputhje me bazën ligjore dhe rregullatore në fuqi. Kjo, për të plotësuar legjislacionin aktualisht në fuqi[10] që parashikon auditimin e databazave shtetërore duke lënë jashtë spektrit të veprimit sistemet në tërësi.

c) Zbatimi i procedurave të qarta sipas të cilave institucionet shtetërore të cilat ofrojnë e - shërbime për qytetarin, biznesin, apo për ndërveprim midis institucionesh do të aksesojnë bazat e të dhënave shtetërore me qëllim ndërveprimin dhe përmirësimin e cilësisë së shërbimit për përfituesit.

d) Forcimi i institucioneve dhe rritja e sigurisë në administratën shtetërore, duke aplikuar procedura dhe kërkesa bazë të gjithëpranuara.

Forcimi i kuadrit institucional

a) Zbatimi i procedurave për mbrojtjen e të dhënave personale të qytetarëve në marrjen e e – shërbimeve.

b) Edukimi dhe ndërgjegjësimi i aktorëve në sektorin publik dhe privat lidhur me kuadrin ligjor dhe rregullativ në fuqi.

c) Krijimi i një sistemi raportues të unifikuar për individët dhe bizneset mbi raportimin e krimit kibernetik në mënyrë që të merren masat e nevojshme si dhe institucionet e forcimit të ligjit të

[10] LIGJ Nr. 10325, datë 23.9.2010 "Për Bazat e të Dhënave Shtetërore" dhe VKM nr. 945, datë 2.11.2012 për miratimin e rregullores "Administrimi i Sistemit të Bazave të të Dhënave Shtetërore"

mund të përcaktojnë shkallën sesa krimi kibernetik në Shqipëri ndikon tek individët dhe në ekonomi.

d) Vlerësimi i krijimit të strukturave të nevojshme respektive pranë institucioneve të tjera të administratës publike. Forcimi dhe mbështetja për rritjen e kapaciteteve në fushën e sigurisë kibernetike do jetë një proces i vazhdueshëm në mënyrë që shteti të shërbejë si model në sigurinë kibernetike.

e) Përcaktimi i qartë i strukturave dhe proceseve të cilat do të sigurojnë koordinimin në nivel politiko-strategjik dhe në nivel operacional duke përfshirë të gjithë aktorët në sektorin publik apo privat.

Rritja e ndërgjegjësimit për sigurinë kibernetike

Botërisht vlerësohet se shumica e sulmeve kibernetike kanë sukses si pasojë e keqkonfigurimit apo mos zbatimit të masave minimale të mbrojtjes nga përdoruesit e TIK.

a) Qeveria do ndërmarrë iniciativa dhe hartojë programe për edukimin dhe ndërgjegjësimin e përdoruesve të TIK. Këto programe do përfshijnë të gjithë nivelet e administratës publike si: specialistët IT, administratorët e sistemeve dhe TIK, etj. Ky proces do të garantojë përdorimin, ngritjen dhe ofrimin e shërbimeve dixhitale të administratës në mënyrë të sigurt dhe të besueshme.

b) Shpërndarja dhe publikimi i informacionit mbi rreziqet e hapësirës kibernetike, nxjerrja e udhëzimeve dhe këshillave për një siguri minimale do jetë një proces i vazhdueshëm nëpërmjet të cilit do synohet të rritet ndërgjegjësimi dhe siguria e përdoruesve të thjeshtë. Përveç publikimit të tyre në faqet zyrtare të internetit të institucioneve të specializuara do bashkëpunohet në mënyrë të ngushtë me median për të siguruar një informim sa më të gjerë dhe të shpejtë të publikut.

c) Vlerësim për futjen e programeve edukative në sistemin arsimor parauniversitar dhe zhvillimi i fushatave të informimit.

d) Bashkëpunimi me sektorin privat si një nga sektorët më të prekshëm nga sulmet kibernetike do forcohet nëpërmjet marrjes të iniciativave dhe projekteve të përbashkëta. Rritja e

ndërgjegjësimit dhe zbatimi i kërkesave minimale të sigurisë do të zbatohet edhe për këtë sektor. Në mënyrë të veçantë ky bashkëpunim do rritet me:

- Ofruesit e shërbimit të internetit, si portat hyrëse të hapësirës kibernetike në vend. Përmes ndërtimit të besimit të ndërsjelltë, bashkëpunimi i ngushtë me ta në baza vullnetare do të rrisë efektivitetin e trajtimit të incidenteve kibernetike duke shkurtuar kohën e përgjigjes; si dhe për të vënë në zbatim masat për bllokimin e aksesit ndaj faqeve të internetit me përmbajtje të paligjshme.
- Shoqërinë civile, për të adresuar çështjet e sigurisë së fëmijëve në internet.
- Akademinë, për të hapur programe studimi të specializuara në siguri kibernetike e për të ngritur fonde duke shfrytëzuar mundësitë si Horizon 2020.
- Sektorin bankar, si një nga sektorët me fjalën e fundit të teknologjisë në drejtim të sigurisë. Përmes komitetit të tyre të sigurisë, ata do të jenë palë në çdo iniciativë ligjore dhe teknike në këtë fushë; si dhe për shkëmbimin e informacionit mbi dobësitë e produkteve dhe teknologjive të TIK, llojet e reja të sulmeve, institucionalizimin e marrëdhënieve, hartimin e planeve të masave dhe veprimeve të koordinuara dhe shkëmbimin e ndërsjelltë të informacionit në lidhje me sulmet kibernetike.

Identifikimi dhe mbrojtja e Infrastrukturave Kritike të Informacionit në Shqipëri

Zhvillimi i teknologjisë dhe integrimi i vazhdueshëm i sistemeve bën që disa sisteme të kthehen në jetike për funksionimin e shoqërisë dixhitale duke i konsideruar ato si infrastruktura kritike.

a) Krijimi i procedurave dhe proceseve të nevojshme për identifikimin, inventarizimin dhe garantimin e sigurisë të tyre. Krijimi dhe implementimi i procedurave dhe kërkesave minimale të sigurisë për këto sisteme do të jetë detyruese.
b) Për shkak se këto sisteme nuk janë vetëm shtetërore, por në të shumtën e rasteve i përkasin sektorit privat, në mënyrë të vazhdueshme do të garantohet siguria bazë e këtyre sistemeve. Lidhur me këtë objektiv një aspekt tjetër mjaft i rëndësishëm përveç mbrojtjes së këtyre sistemeve kritike është "aftësia ripërtëritëse" (*resilience*) e cila mundëson garantimin e vazhdueshmërisë së biznesit në rastet e ndodhjes së forcave madhore apo të sulmeve të ndryshme kibernetike. Mbrojtja dhe aftësia ripërtëritëse e infrastrukturave kritike si dhe inkurajimi i operatorëve që i zotërojnë ato për implementimin e një arkitekture sigurie të

plotë (përfshirë menaxhimin e riskut dhe të emergjencave) do të garantojë efektivitetin, besueshmërinë dhe vazhdueshmërinë e shërbimeve të ofruara prej tyre.

c) Përcaktimi i bazës ligjore/rregullative mbi të cilën operatorët e infrastrukturave kritike do të duhet të raportojnë mbi incidentet e rënda kibernetike. Për çdo rast (të evidentuar ose jo) si krim kibernetik duhet të bëhet analiza e tij, shkaqet e ndodhjes dhe nxjerrja e detyrave që duhet të reflektohen në akte ligjore apo rregullore e procedura për eliminimin e përsëritjes së rastit.

Krijimi dhe implementimi i kërkesave minimale të sigurisë kibernetike

Rritja e sigurisë së pari në administratën shtetërore, rritja e përdorimit të sistemeve TIK në administratën shtetërore por dhe garantimi i sigurisë të tyre është një nga prioritetet e këtij Dokumenti.

a) Standarde, udhëzime dhe procedura të bazuara në praktikat më të mira ndërkombëtare duhet të përshtaten dhe miratohen për t'u zbatuar në administratën shtetërore.

b) Krijimi dhe miratimi i procedurave të analizës të rrezikut të sigurisë për sistemet e përdorura dhe shërbimet elektronike të ofruara nga institucionet është prioritet. Analiza e rrezikut do të jetë një proces i vazhdueshëm dhe do kryhet në mënyrë periodike. Zbatimi i tyre do jetë një nga elementët kyç për rritjen e nivelit të sigurisë kibernetike.

c) Zhvillimi i mëtejshëm i procedurave për koordinimin e investimeve me synim analizimin e sigurisë dhe harmonizimin e projekteve që në fazat e projektimit.

d) Do të identifikohen sistemet e rëndësishme në administratën shtetërore dhe institucionet do të investojnë në hardware dhe software të automatizuara si masa proaktive dhe reaktive për të siguruar këto sisteme që administrojnë.

e) Do të ngrihen BCC (Business Continuity Center) dhe DRC (Disaster Recovery Center) për rrjetet/sistemet shtetërore.

f) Do të ngrihet një sistem monitorimi, i cili do t'i njoftonte në kohë institucionet për rreziqet kibernetike që u kanosen duke monitoruar 24\7 nyjet më të rëndësishme, trafikun dhe eventet që ndodhin në sistem për të mundësuar edhe nxjerrjen e konkluzioneve nga logg-et që ruhen, pa ndërhyrë apo monitoruar përmbajtjen.

Forcimi i partneritetit me struktura të tjera përgjegjëse të fushës brenda dhe jashtë vendit

Koordinimi dhe bashkëpunimi i të gjithë aktorëve është elementi bazë për garantimin e suksesit. Për shkak të dinamikës dhe shpejtësisë me të cilën zhvillohet TIK bashkëpunimi me sektorin privat do të forcohet. Vetëm nëpërmjet një bashkëpunimi të ngushtë mund të rritet siguria dhe zhvillimi i TIK në administratën shtetërore në koherencë me zhvillimet dhe trendin e teknologjisë.

a) Rritja e bashkëpunimit dhe koordinimit ndërmjet institucioneve shtetërore do të forcohet për të garantuar ndërveprimin dhe koordinimin në forcimin e sigurisë dhe minimizimin e dëmeve nga sulmet kibernetike.

b) Shqipëria mbështet dhe do të jetë pjesë e iniciativave ndërkombëtare të cilat synojnë rritjen dhe forcimin e sigurisë. Në mënyrë të veçantë do të forcohet bashkëpunimi me NATO dhe BE-në duke u bërë pjesë aktive e iniciativave të përbashkëta për sigurinë kibernetike. Anëtarësimi i Shqipërisë në organizmat dhe shoqatat e sigurisë kibernetike të njohura ndërkombëtare dhe rritja e bashkëpunimit është prioritet.

Rritja e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike

Në afatshkurtër dhe afatmesëm, do të realizohen aktivitete me qëllim ngritjen e kapaciteteve të burimeve njerëzore të nevojshme në fushën e sigurisë kibernetike. Do të krijohen rregullore për të përfshirë konceptin e sigurisë kibernetike në programet e shkollave fillore, shkollave të mesme, dhe të institucioneve të arsimit të lartë. Do të diskutohen gjithashtu hapat e auditimit mbi sigurinë kibernetike në proceset e auditimit të brendshëm të organizatave.

a) Në kuadër të forcimit të institucioneve, do të rriten kapacitetet teknike të burimeve njerëzore. Kjo do të bëhet përmes programeve të zgjedhura të trajnimeve të cilat do të synojnë aftësimin e pjesëmarrësve në parandalimin e sulmeve, minimizimin e dëmeve, dhënien e përgjigjes efektive ndaj incidenteve të sigurisë së informacionit.

b) Pjesëmarrja aktive në konferenca ndërkombëtare, takime, seminare dhe ushtrime që kanë të bëjnë me sigurinë kibernetike. Shkëmbimi i informacioneve, analizave, eksperiencave, krijimi i projekteve të përbashkëta, vlerësimi i teknologjive dhe sistemeve të sigurisë shihen jo vetëm si një mundësi për rritjen e sigurisë kibernetike në institucionet publike,

por dhe si një investim për zhvillimin dhe rritjen e kapaciteteve të brezave pasardhës.

Analiza SWOT (strength, weakness, opportunities, threats)

Për hartimin e këtij dokumenti është hartuar një analizë SWOT që lidhet me pikat e forta, të dobëta, mundësitë dhe kërcënimet që mund të ndikojnë në mosrealizimin e suksesshëm të saj.

Fortësitë	**Dobësitë**
a. Përqasje që synon të forcojë bashkëpunimin ndërmjet Qeverisë me operatorët e Infrastrukturave Kritike të Informacionit b. Institucione të angazhuara për implementimin e Dokumentit të Politikave si dhe institucione gjithmonë më të ndërgjegjësuara për rreziqet që i kanosen hapësirës kibernetike; c. Plan veprimi i struktuar me mekanizma të qarta që do të lejojnë monitorim të zbatimit të këtij Dokumenti.	a. Mungesë historiku në fushën e sigurisë kibernetike: i. Mungesë strategjie në nivel kombëtar në këtë fushë deri më tani; ii. Mungesë kuadri rregullator. b. Nevojë për investime madhore për të arritur nivele të krahasueshme me rajonin dhe BE, deri më tani siguria nuk theksohej që në fazat fillestare të ngritjes së infrastrukturave të TIK; c. Kuadri ekzistues ligjor dhe institucional ka nevojë për t'u plotësuar d. Mungesë e profesionistëve të specializuar dhe të certifikuar për sigurinë kibernetike; e. Nivel i ulët i kulturës së navigimit të sigurtë në internet në popullatë .
Mundësitë	**Kërcënimet**
a. Janë ngritur tashmë struktura përgjegjëse në hallka të ndryshme të procesit të menaxhimit të sigurisë kibernetike; b. Akses në praktikat më të mira ndërkombëtare dhe mundësi për t'u mbështetur në dokumenta strategjike rajonale si dhe të partnerëve evropianë e të NATO-s;	a. Mungesë koordinimi dhe vullneti për të përmbushur detyrimet; b. Fragmentizimi i burimeve dhe mbivendosja e investimeve.

d. Investimet nga ana e Qeverisë në fushën e TIK janë gjithnjë e në rritje si në pikëpamje të teknologjisë ashtu edhe të burimeve njerëzore.	

Llogaridhënia, monitorimi dhe analiza vlerësuese

Formimi i sigurisë kibernetike në kushtet e një teknologjie informacioni që ndryshon dita ditës kërkon vëmendje të veçantë nga ana e institucioneve publike. Ato duhet të përcaktojnë kushtet e nevojshme dhe mënyrat për të përshpejtuar procesin e përfshirjes aktive të sektorit privat dhe publik për të diskutuar politikat e këtij Dokumenti si dhe zbatimin me efikasitet të tyre.

Institucionet Qeveritare luajnë një rol udhëheqës në termat e:

1. Plotësimit të kuadrit ligjor në fushën e sigurisë kibernetike;
2. Identifikimin dhe mbrojtjen e Infrastrukturave Kritike të Informacionit (CIIP);
3. Krijimin dhe implementimin e kërkesave bazë të sigurisë kibernetike;
4. Shtimin i investimeve për rritjen e sigurisë në rrjetet/sistemet shtetërore;
5. Forcimin e partneritetit me struktura të tjera përgjegjëse të fushës brenda dhe jashtë vendit;
6. Rritjen e ndërgjegjësimit për sigurinë kibernetike;
7. Rritjen e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike.

Institucionet qeveritare duhet të krijojnë parakushtet si dhe duhet të nxisin sektorin privat, OJQ-të dhe veçanërisht operatorët e infrastrukturave kritike të informacionit që:

- Të marrin pjesë në procesin e përmirësimit të kuadrit ligjor në fushën e sigurisë kibernetike;
- Të jenë aktiv në procesin e identifikimit të infrastrukturave kritike të informacionit;
- T'i kushtojnë një rëndësi të veçantë rritjes së kapaciteteve njërëzore;
- Marrin pjesë aktivisht në përcaktimin e kërkesave minimale të sigurisë kibernetike;
- Pjesëmarrjen në takimet me përfaqësues të institucioneve shtetërore dhe private për të zgjidhur çështje të rëndësishme;
- Paraqitjen e projekteve dhe pjesëmarrjen në diskutimet publike mbi legjislacionin;
- Të marrin pjesë në partneritete publik – privat;
- Rritjen e pjesëmarrjes në monitorimin e rezultateve të këtij Dokumenti Politikash.

Ky dokument politikash do të monitorohet nga Grupi Ndërinstitucional i Punës për Hartimin e "Dokumentit të Politikave për Sigurinë Kibernetike", i ngritur me urdhër të Kryeministrit nr. 120, datë 20.03.2014, Ministri përgjegjës për Administratën Publike dhe Inovacionin, Agjencia

Kombëtare për Sigurinë Kompjuterike (ALCIRT) si dhe Departamenti i Programimit të Zhvillimit, Financimeve dhe Ndihmës së Huaj pranë Këshillit të Ministrave.

Parakushtet për zbatimin efikas dhe me sukses të "Dokumentit të Politikave për Sigurinë Kibernetike 2015 – 2017" përfshijnë:

- Konsensusin e përgjithshëm dhe vullnetin e mirë për të zbatuar objektivat dhe aktivitetet e propozuara;
- Promovimi i "Dokumentit të Politikave për Sigurinë Kibernetike 2015 – 2017" si dhe objektivave të tij si ndaj sektorit publik, privat dhe qytetarëve;
- Një sistem i monitorimit dhe vlerësimit efikas për të kontrolluar nëse objektivat e përcaktuara në Dokumentin e Politikave janë realizuar;
- Nxitja e bashkëpunimit ndërmjet autoriteteve shtetërore si dhe njohja e vazhdueshme me praktikat më të mira të rajonit.

Zbatimi i këtij dokumenti politikash do të bazohet në përdorimin e një numri treguesish të lidhur me inputet, proceset, produktet dhe efektet e planit të veprimit. Treguesit do të vlerësohen në mënyrë periodike nga institucionet publike sipas ndarjes së punës dhe sferës së tyre të juridiksionit në fushën e sigurisë kibernetike. Treguesit do të mblidhen nga ALCIRT përkatësisht sipas treguesve të paracaktuar në këtë dokument për përmbushjen e çdo politike në bashkëpunim me institucionet e ndryshme publike. Bazuar në këto tregues Ministri përgjegjës për Administratën Publike dhe Inovacionin do të prodhojë raporte vjetore të ecurisë së dokumentit të politikave të cilat do të jetë publike.

Ngritja e një sistemi monitorimi dhe vlerësimi efektiv do të mbështetet nga aktivitete të forcimit të kapaciteteve njerëzore dhe strukturore si dhe investim në infrastrukturat e TIK më të sigurta. Informimi i publikut, si dhe monitorimi i zbatimit të dokumentit të politikave dhe rezultateve të tij nga shoqëria civile si dhe operatorët e sektorit privat do të përbëjnë gjithashtu një nga elementet bazë të sistemit të monitorimit dhe llogaridhënies.

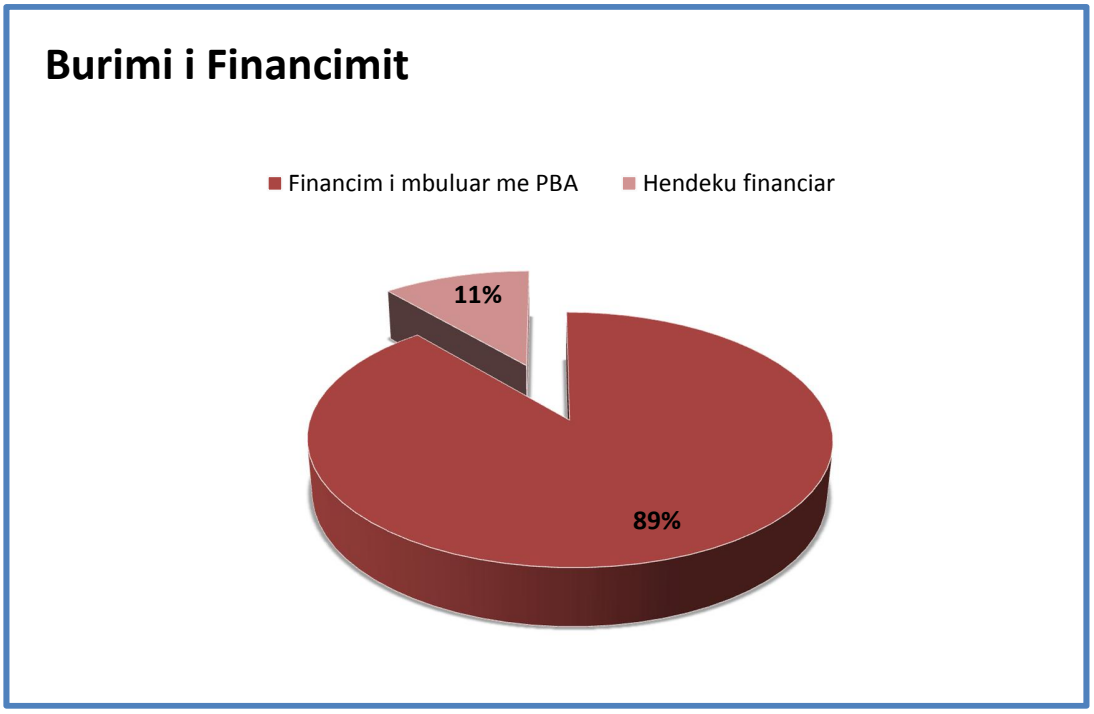
Financimi i Dokumentit të Politikave

Përcaktimi i nevojave të financimit të "Dokumentit të Politikave për Sigurinë Kibernetike 2015 – 2017" u realizua nëpërmjet procesit të vlerësimit të kostove potenciale të nevojshme, nga secili institucion i përfshirë në këtë Dokument. Çdo institucion ka përgjegjësinë kryesore në realizimin e aktiviteteve të parashikuara në planin e veprimit që shoqëron këtë Dokument.

Fondet e vlerësuara të nevojshme për zbatimin e aktiviteteve të detajuara në planin e veprimit të këtij Dokumenti gjatë periudhës kohore 2015 – 2017 parashikohet të jenë 626,909,833 lekë.

Objektivat strategjike të Dokumentit	Kostot e vlerësuara
OBJ.1. Plotësimi i kuadrit ligjor në fushën e sigurisë kibernetike	Kosto të funksionimit të institucioneve
OBJ. 2. Forcimi i kuadrit institucional	Kosto të funksionimit të institucioneve
OBJ. 3. Rritja e ndërgjegjësimit për sigurinë kibernetike	1,120,000 ALL
OBJ. 4. Identifikimi dhe mbrojtja e Infrastrukturave Kritike të Informacionit në Shqipëri	Kosto të funksionimit të institucioneve
OBJ. 5. Krijimi dhe implementimi i kërkesave minimale të sigurisë kibernetike	Kosto të funksionimit të institucioneve dhe 618,439,833 ALL
OBJ. 6. Forcimi i partneritetit me struktura të tjera përgjegjëse të fushës brenda dhe jashtë vendit	Nuk janë vlerësuar kosto
OBJ. 7. Rritja e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike	7,350,000 ALL

Duhet theksuar se nevojat për financimin e zbatimit të Dokumentit të Politikave janë llogaritur për zbatimin e aktiviteteve për periudhën 2015-2017, por duhet theksuar se në tërësinë e aktiviteteve të parashikuara, një pjesë e tyre, përkatësisht aktivitetet që i shërbejnë realizimit të objektivave 1, 2, 4 dhe 6 nuk mund të përcaktohen në këtë fazë, pasi ata janë aktivitete, fillimi i të cilëve varet tëresisht nga përfundimi i aktiviteteve paraprake ku përmendim: plotësim kuadri ligjor, varësi nga përfundimi i punës së ndonjë Grupi Ndërinstitucional Pune për këtë qëllim, ose sepse këto aktivitete realizohen me punën e punonjësve të institucioneve dhe janë pjesë e detyrave të tyre të kohëpaskohëshme, etj. Burimi i financimit për këtë Dokument është Buxheti i Shtetit (me PBA). Kosto e vetme e pambuluar nga PBA-ja dhe/ose donatorët është vlera prej 70,000,000 lekë e parashikuar për 'Krijimin e Infrastrukturës për sistemin e monitorimit dhe atë të mbrojtjes (ISMS), pra rreth 11,1%, i përcaktuar si aktivitet për plotësimin e objektivit strategjik të pestë.



Megjithatë, kostimi i "Dokumentit të Politikave për Sigurinë Kibernetike 2015 – 2017" do të jetë objekt rishikimi vjetor njëlloj si edhe vetë Dokumenti në mënyrë që të reflektohet qartë plani i financimeve dhe realizimi faktik i tyre.