AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE
DREJTORIA E KOORDINIMIT TË PROJEKTEVE NDËRKOMBËTARE DHE ZHVILLIMIT STRATEGJIK TË SIGURISË KIBERNETIKE

RAPORT MONITORIMI I STRATEGJISË KOMBËTARE PËR SIGURINË KIBERNETIKE 2020-2025

VITI 2024

Tiranë, 2025

Adresa: Rruga "Papa Gjon Pali II", Nr. 3, Kati 1, Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax: 04 2221 039

Përmbajtja

Tabela e Grafikëve

I. SHKURTIME

SKSK	Strategjia Kombëtare për Sigurinë Kibernetike
AKSK	Autoriteti Kombëtar për Sigurinë Kibernetike
CSIRT	*Computer Security Incident Response Teams*- Ekipet e Reagimit ndaj Incidenteve të Sigurisë Kompjuterike
NATO	Organizata e Traktatit të Atlantikut të Veriut
PBA	Programi Buxhetor Afatmesëm
SOC	*Security Operations Center*- Qendra Operacionale e Sigurisë
LEA	*Law Enforcement Agencies*- Agjencitë Ligjzbatuese
CERT	*Computer Emergency Response Team*- Ekipi për Reagim Emergjent ndaj Incidenteve Kompjuterike
OSBE	Organizata për Siguri dhe Bashkëpunim në Evropë
QKEDH	Qendra Kundër Ekstremizmit të Dhunshëm
UNDP	*United Nations Development Programme*- Programi i Kombeve të Bashkuara për Zhvillim
UNICEF	*United Nations Children's Fund*- Fondi i Emergjencës i Kombeve të Bashkuara për Fëmijet
NJMF	Njësia e Mbrojtjes së Fëmijëve

Parahyrje

Ky raport monitorimi është hartuar duke u bazuar në kontributin e dhënë nga strukturat brenda Autoritetit, si dhe institucionet përgjegjëse për zbatimin e Planit të Veprimit të dakordësuar për vitin 2024.

Raporti është pjesë e raportimeve vjetore për zbatimin e Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025, të publikuara në faqen zyrtare të Autoritetit Kombëtar për Sigurinë Kibernetike www.aksk.gov.al dhe përfshin periudhën Janar- Dhjetor 2024.

I. HYRJE

Siguria kibernetike është pjesë integrale e sigurisë së qytetarëve. Me mbi 95% të shërbimeve publike të digjitalizuara, varësia nga sistemet e informacionit dhe pajisjet teknologjike është rritur ndjeshëm, duke e bërë hapësirën digjitale të Republikës së Shqipërisë më të ekspozuar ndaj kërcënimeve kibernetike.

Sulmet ndaj infrastrukturave kritike nuk janë më vetëm sfida teknologjike, por përfaqësojnë rrezik të drejtpërdrejtë kombëtar, që cenojnë aksesin në shërbime bazë dhe përfitimet që sjell interneti për qytetarët dhe ekonominë. Ndaj, ndërtimi i një ekosistemi të sigurt dhe të qëndrueshëm kibernetik është më shumë se një nevojë teknike, është një domosdoshmëri strategjike për të garantuar mirëqenie, siguri dhe besim në epokën digjitale.

Në mbështetje të objektivave të qeverisë shqiptare, transformimit digjital dhe përdorimit të sigurt të internetit, Autoriteti Kombëtar për Sigurinë Kibernetike ka zbatuar Strategjinë Kombëtare për Sigurinë Kibernetike (SKSK) 2020-2025, miratuar me Vendimin nr. 1034, datë 24.12.2020.

Kjo strategji mbështetet në parimet themelore të mëposhtme:

- Zbatimi i vlerave të njëjta themelore në botën fizike dhe digjitale;
- Mbrojtja e të drejtave themelore, liria e shprehjes, të dhënat personale dhe privatësia;
- Qasja për të gjithë;
- Qeverisje demokratike dhe efikase;
- Përgjegjësi e përbashkët në garantimin e sigurisë kibernetike.

Me qëllim zbatimin dhe vlerësimin periodik të SKSK 2020-2025, AKSK harton raportin vjetor të monitorimit sipas kontributit nga secili institucion përgjegjës.

Aktorët e zbatimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025 janë:

- Autoriteti Kombëtar për Sigurinë Kibernetike;
- Ministria e Brendshme;
- Ministria e Infrastrukturës dhe Energjisë;
- Drejtoria e Përgjithshme e Policisë së Shtetit;
- Autoriteti Kombëtar për Sigurimin e Informacionit të Klasifikuar;
- Qendra për Koordinimin Kundër Ekstremizmit të Dhunshëm;
- Agjencia Kombëtare e Shoqërisë së Informacionit;
- Ministria e Shëndetësisë dhe Mbrojtjes Sociale;
- Ministria e Arsimit dhe Sportit;
- Autoriteti i Komunikimeve Elektronike dhe Postare;
- Agjencia Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijës.

Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025 ka parashikuar për zbatim 4 (katër) Politika, 14 (katërmbëdhjetë) Objektiva Specifik, 47 (dyzetë e shtatë) Masa dhe ky raport paraqet një analizë të thellë mbi progresin dhe realizimin e tyre gjatë vitit 2024.

Kjo Strategji synon realizimin e qëllimeve të katër politikave, si vijon:

Qëllimi i politikës 1: *Garantimi i sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit, duke fuqizuar mjetet teknologjike dhe juridike.*

Qëllimi i politikës 2: *Ndërtimi i një mjedisi të sigurt kibernetik, duke edukuar dhe ndërgjegjësuar shoqërinë në ngritjen e kapaciteteve profesionale në fushën e sigurisë së informacionit*

Qëllimi i politikës 3: *Krijimi i mekanizmave të nevojshëm për sigurinë e fëmijëve në hapësirën kibernetike, duke përgatitur njëkohësisht brezin e ri të aftë për të përfituar nga përparësitë e teknologjisë së informacionit dhe për të përballuar sfidat e zhvillimit*

Qëllimi i politikës 4*: Rritja e bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike me partnerët strategjikë*

Siç paraqitet edhe në mënyrë më të gjerë në këtë raport monitorimi, gjatë kësaj periudhe janë shënuar një sërë zhvillimesh dhe arritjesh të rëndësishme në fushën e sigurisë kibernetike, në kuadër të përmbushjes së katër qëllimeve të politikave, ku secili institucion raporton mbi nivelin e zbatimit të secilit objektiv dhe masë, mbi buxhetin e alokuar, problemet e hasura dhe vlerësimin e progresit të strategjisë në përgjithësi. Me qëllim monitorimin e zbatueshmërisë së masave të SKSK gjatë kësaj periudhe është marrë në konsideratë i njëjti vit, ku nga monitorimi i detajuar i zbatimit të masave të parashikuara në SKSK 2020-2025, për vitin 2024 rezulton se:

Për periudhën raportuese është parashikuar fillimi i zbatimit të katër politikave, 14 Objektivave Specifikë dhe 48 Masa, nga të cilat 16 Masa për Politikën 1, 8 Masa për Politikën 2, 19 Masa për Politikën 3 dhe 5 Masa për Politikën 4.

Raporti i monitorimit të SKSK 2020–2025, për periudhën 1 Janar - 31 Dhjetor 2024, është hartuar mbi bazën e kontributit të dhënë nga institucionet përgjegjëse dhe ato shpenzuese të përfshira në zbatimin e kësaj Strategjie.

II. METODOLOGJIA E PËRDORUR PËR HARTIMIN E RAPORTIT TË MONITORIMIT DHE PERFORMANCËS

Metodologjia e përdorur për hartimin e Raportit të Monitorimit përshkruan procesin e ndjekur gjatë hartimit të raportit duke pasur synim kryesor mundësimin e udhëzimeve të qarta, që lehtësojnë kuptueshmërinë e tij dhe orientimin drejt paraqitjes së rezultateve kryesore. Kjo metodologji synon të evidentojë arritjet, sfidat dhe rekomandimet për përmirësim, duke i shërbyer një procesi të mirëfilltë monitorimi të bazuar në rezultate të prekshme.

Për të garantuar një monitorim efektiv dhe të saktë, Autoriteti Kombëtar për Sigurinë Kibernetike ka bashkëpunuar në mënyrë të vazhdueshme me institucionet e përfshira këtë Strategji, duke dakordësuar në zbatimin e një Plani Veprimi, të përshtatur sipas natyrës dhe specifikave të çdo strukture, me qëllim sigurimin e informacionit të saktë dhe gjithëpërfshirës për procesin e raportimit si më poshtë vijon:

a. Nivelin e zbatimit të çdo mase (aktivitetet e realizuara për vitin 2024, në proces, si dhe nje përshkrim të aktiviteteve të realizuara ose një argumentim për mosrealizimin apo realizimin e pjesshëm të tyre);

b. Masën e buxhetit të realizuar në raport me çfarë është parashikuar për realizim e masës në përputhje me objektivat;

c. Informacion mbi realizimin e deritanishëm për aktivitetet në proces (masa në % e realizimit) dhe parashikimin për përmbylljen e tyre;

d. Informacion mbi % e buxhetit të shpenzuar për aktivitetet në proces;

e. Parashikimi për aktivitetet të cilat rezultojnë të parealizuara ende.

Zbatueshmëria e masave dhe aktiviteteve të Planit të Veprimit të dakordësuar klasifikohet me vlerat si më poshtë:

Vlera	Përshkrimi
E realizuar	**Masa/aktivitete të cilat janë përmbushur**
Realizuar Pjesërisht/ Në proces	Masa/aktivitete, të cilat në periudhën e raportimit kanë pasur zbatim të pjesshëm dhe/apo që vijojnë të jenë në proces zbatimi nga institucionet përgjegjëse
E parealizuar	Të pazbatuara janë raportuar ato masa/aktivitete, të cilat nuk kanë regjistruar zhvillim për periudhën raportuese si dhe gjithashtu ato masa/aktivitete për të cilat nuk është dhënë raportim nga strukturat/institucionet përgjegjëse.

Në këtë mënyrë AKSK ka kryer identifikimin e aktiviteteve të cilat kanë sjellë rezultate të dukshme në përmbushjen e objektivave, gjithashtu evidentimin e sfidave, problematikave dhe faktorëve që kanë ndikuar progresin apo zbatimin e masave të parashikuara në dokumentet strategjik.

III. MASA TË IMPLEMENTUARA ME SUKSES NË VITIN 2024

Viti 2024 ka shënuar një sërë arritjesh të rëndësishme, pozitive dhe inkurajuese në fushat kryesore të Strategjisë Kombëtare për Sigurinë Kibernetike (SKSK), të cilat janë përkthyer në rezultate konkrete dhe kanë pasur impakt të ndjeshëm në zbatimin e katër Politikave të saj. Krahas këtyre arritjeve, janë evidentuar edhe disa sfida të cilat kanë ndikuar në performancën e disa objektivave specifikë të strategjisë. Masat dhe aktivitetet e mëposhtme, reflektojnë hapat dhe projektet specifike të ndërmarra në funksion të zbatimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025 për periudhën referuese 1 Janar 2024-31 Dhjetor 2024, grupuar sipas politikave:

A. QËLLIMI I POLITIKËS 1

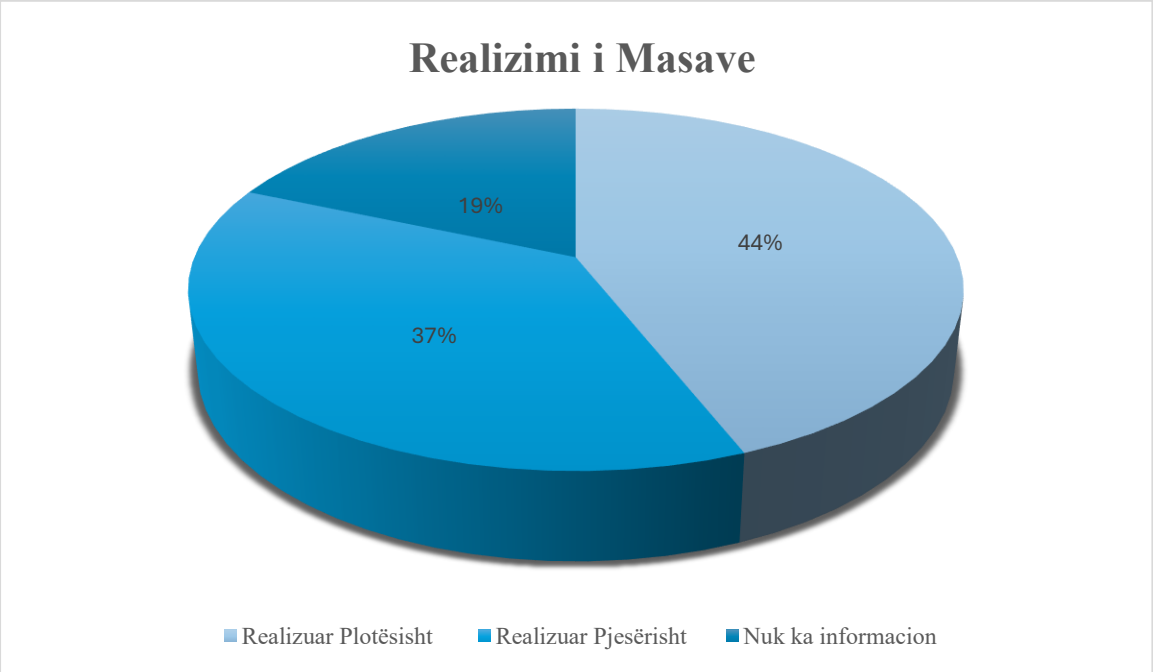
Garantimi i sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit, duke fuqizuar mjetet teknologjike dhe juridike.

Objektivat e politikës fokusohen në:

- Përmirësimi i kuadrit ligjor që normon dhe rregullon fushën e sigurisë kibernetike në vend, si dhe harmonizimi i tij me direktivat dhe rregulloret e Bashkimit Evropian;
- Ngritja dhe funksionimi i CSIRT-eve në të gjithë sektorët e industrisë në nivel kombëtar;
- Fuqizimi dhe implementimi i masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit;
- Përmirësimi i infrastrukturave të informacionit për të luftuar krimin kibernetik, radikalizimin dhe ekstremizmin e dhunshëm.

Gjatë vitit 2024, Plani i Veprimit i dakordësuar me institucionet për Politikën 1, parashikon zbatimin e gjithsej 16 masave. Nga të cilat, siç vërehet edhe nga Grafiku 1:

- 44 % e Masave janë realizuar plotësisht;
- 37.5% e Masave janë realizuar pjesërisht;
- 18.5% e Masave nuk ka informacion.



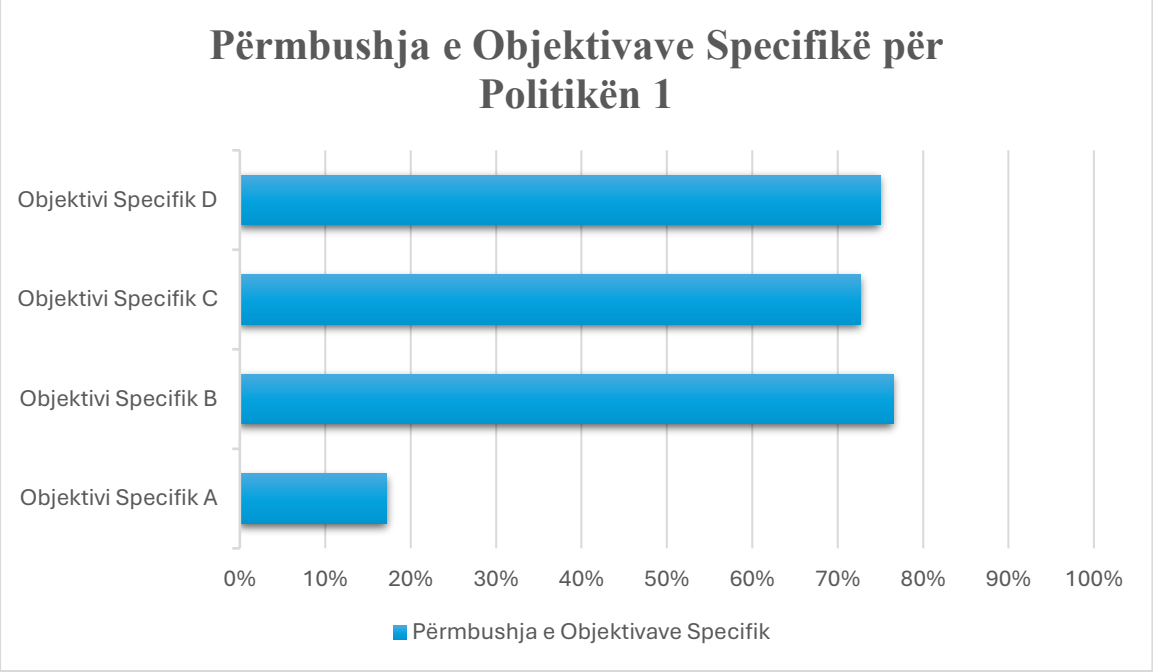
Grafiku 1. Realizimi i Masave të Politikës 1

Përsa i përket përmbushjes së Objektivave Specifikë të kësaj Politike:

- **Objektivi Specifik A**: Përmirësimi i kuadrit ligjor që normon dhe rregullon fushën e sigurisë kibernetike në vend, si dhe harmonizimi i i tij me direktivat dhe rregulloret e Bashkimit Europian.
- **Objektivi Specifik B**: Ngritja dhe funksionimi i CSIRT-eve në të gjithë sektorët e industrisë në nivel kombëtar.
- **Objektivi Specifik C:** Fuqizimi dhe implementimi i masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit.
- **Objektivi Specifik D**: Përmirësimi i infrastrukturave të informacionit për të luftuar krimin kibernetik, radikalizimin dhe ekstremizmin e dhunshëm.

është vlerësuar se:

- Objektivi Specifik A është realizuar në masën 17.8 %;
- Objektivi Specifik B është realizuar në masën 76.5%;
- Objektivi Specifik C është realizuar në masën 72.7%;
- Objektivi Specifik D është realizuar në masën 75%.



Grafiku 2. Përmbushja e Objektivave Specifikë për Politikën 1

Ndër rezultatet kryesore të arritura, në kuadër të përmbushjes së masave të parashikuara në Planin e Veprimit të dakordësuar, në lidhje me këtë Politikë janë:

- Përmirësimi i Metodologjisë për Identifikimin dhe Klasifikimin e Infrastrukturave Kritike dhe të Rëndësishme të Informacionit;

- Ndryshimi i VKM Nr. 141 datë 22.02.2017 "Për organizimin e Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike";
- Legjislacioni i përafruar dhe i miratuar Për Sigurinë Kibernetike;
- Implementimi i standardeve ndërkombëtare për menaxhimin e sigurisë së informacionit;
- Testimi i sigurisë së sistemeve dhe aplikacioneve në administrimin e AKSK;
- Përfshirje aktive në takimet periodike me iniciativë të NATO-s;
- Thellimi i bashkëpunimit me NATO-n, për reagimin ndaj incidenteve të sigurisë kibernetike, shkëmbimin e ekspertizës teknike dhe informacionit, në lidhje me kërcënimet dhe dobësitë;
- Pjesëmarrja në ushtrimet kibernetike të përbashkëta që organizon NATO e koordinuar me institucionet kombëtare të sigurisë dhe të mbrojtjes;
- Ngritja e Qendrës Kombëtare Operacionale (SOC Kombëtar) për monitorimin proaktiv dhe reaktiv dhe trajtimin e incidenteve kibernetike;
- Investime në platforma teknologjike për rritjen e sigurisë kibernetike (pa *hardware*);
- Miratimi dhe përditësimi i procedurave për trajtimin dhe menaxhimin e incidenteve kibernetike;
- Përmirësimi i infrastrukturave të informacionit (pajisje *software* dhe *hardware*). Ngritja e sistemit të kontrollit të aksesit në rrjetin Gov NET;
- Analizë teknike e raporteve të konformitetit nga palët e treta mbi përputhshmërinë e kërkesave ligjore dhe teknike për infrastrukturat kritike dhe të rëndësishme;
- Organizimi i fushatave sensibilizuese në shkolla dhe me qasje në komunitet "Kundër radikalizimit dhe ekstremizmit të dhunshëm online" me target grupe të ndryshme sipas profilit dhe portofolit të Ministrive të Linjës, institucioneve të varësisë si dhe pushtetit vendor;
- Rritja e aftësive për monitorim, parandalim, dhe kundërpërgjigje ndaj përhapjes së përmbajtjeve me gjuhë urrejtje, diskriminuese, të dhunshme dhe esktemiste në internet.

Vijojnë të mbeten në proces realizimi masat dhe aktivitetet si më poshtë:

- Përmirësimi i kuadrit rregullator për sigurinë kibernetike i harmonizuar me ligjet sektoriale, për të adresuar saktë çështjet dhe zgjidhur ato duke perfshire, por pa u kufizuar: Cloud computing, ICT, teknologjine 5G, Inteligjencen Artificiale;
- Përshtatja e vazhdueshme e standardeve dhe rregullave sipas zhvillimeve të fushës, së sigurisë kibernetike;
- Ngritja e CSIRT-it Kombëtar dhe CSIRT-ve të reja sektoriale, në infrastrukturat kritike dhe të rëndësishme të informacionit, si dhe fuqizimi i atyre ekzistuese;
- Krijimi i kushteve optimale të punës për funksionimin e CSIRT-eve, në përmbushje të detyrave të veta, për të garantuar sigurinë kibernetike në infrastrukturat kritike e të rëndësishme të informacionit;
- Përdorimi i AI në dhënien e shërbimeve publike elektronike të sigurta;

Në tërësi, shkalla e zbatimit të Politikës 1 për periudhën raportuese 1 Janar - 31 Dhjetor 2024 është vlerësuar në 52[1]%, bazuar në ecurinë e masave të ndërmarra.

INFORMACION MBI ZBATIMIN E MASAVE:

- AKSK ka pasur rolin drejtues në zbatimin e Strategjisë Kombëtare të Sigurisë Kibernetike të Shqipërisë. Në vitin 2024 u miratua Ligji Nr. 25/2024 "Për Sigurinë Kibernetike", i cili ka sjellë një sërë risish dhe zhvillimesh të rëndësishme siç është krijimi i Qendrës Kombëtare Operacionale të Sigurisë Kibernetike (SOC) që monitoron dhe menaxhon sigurinë kibernetike në nivel kombëtar. Gjithashtu, ligji parashikon ngritjen e një strukture për trajtimin e situatave emergjente dhe menaxhimin e krizave kibernetike, e cila do të menaxhohet nga Ekipi i Përgjigjes ndaj Emergjencave të Sigurisë Kibernetike (CERT). Ky ekip ka për qëllim të ofrojë një përgjigje të shpejtë dhe efikase ndaj incidenteve kibernetike, duke minimizuar pasojat për sektorët e ndryshëm dhe për shoqërinë në përgjithësi.

  Një element tjetër i rëndësishëm ishte garantimi i sigurisë kibernetike përmes rregullimit të certifikimit në përputhje me skemat e BE-së, duke siguruar certifikimin dhe përmirësimin e mbrojtjes nga rreziqet kibernetike për institucionet dhe operatorët e infrastrukturave të informacionit. Përgjatë vitit 2024 janë hartuar dhe miratuar aktet nënligjore si më poshtë:

- *VKM Nr. 783, datë 18.12.2024, "Për organizimin dhe funksionimin e Autoritetit Kombëtar për Sigurinë Kibernetike"*
- *VKM Nr. 683, datë 6.11.2024, "Për miratimin e metodologjisë për identifikimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit"*
- *Rregullore mbi Mënyrën e Dokumentimit dhe Implementimit të Masave të Sigurisë në Infrastrukturat Kritike dhe të Rëndësishme të Informacionit (Miratuar me Urdhër Nr. 97, datë 05.03.2024)*
- *Rregullore për Kategorizimin e Incidenteve të Sigurisë Kibernetike (Miratuar me Urdhër Nr.299, datë 21.08.2024)*
- *Rregullore për Mënyrat dhe Afatet e Ruajtjes së Log-eve të Incidenteve të Sigurisë Kibernetike (Miratuar me Urdhër Nr.408, datë 07.11.2024)*
- *Rregullore për Procedurat e Menaxhimit të Incidenteve të Sigurisë Kibernetike, Kundërmasat dhe Playbooks (Miratuar me Urdhër Nr.1089, datë 18.12.2024)*

  Gjithashtu, përmes trajnimeve, ushtrimeve, bashkëpunimit dhe teknologjive moderne, njësitë e AKSK-së kanë forcuar kapacitetet operacionale, kanë ndërtuar partneritete të qëndrueshme, kanë mbrojtur infrastrukturën kritike dhe kanë reaguar me sukses ndaj kërcënimeve. Kontributi i tyre ka rritur sigurinë dhe rezistencën kibernetike të vendit, duke e pozicionuar Shqipërinë si një shembull të përparimit në këtë fushë. Mbrojtja e

[1] *Kjo përqindje vjen si rezultat i mungesës së informacionit, ku Objektivi Specifik A zë një peshë të madhe, e si rrjedhojë ul përqindjen.. Llogaritur me mesatare të ponderuar (17.8%×0.4)+(76.5%×0.2)+(72.7%×0.2)+(75%×0.2)=51.96%*

infrastrukturave kritike ka qenë një prioritet strategjik për të garantuar funksionimin e pandërprerë të sistemeve dhe për të minimizuar rreziqet ndaj shërbimeve publike dhe private[2].

Autoriteti Kombëtar për Sigurinë Kibernetike ka ndërmarrë një sërë iniciativash për të rritur nivelin e aftësive operacionale të SOC dhe *Red Team*, duke i mundësuar këtyre ekipeve të përballojnë me sukses sfidat e sigurisë kibernetike dhe të përmbushin objektivat e Strategjisë Kombëtare. Kjo është arritur përmes një qasjeje të strukturuar që kombinon trajnimet e specializuara, ushtrimet praktike dhe adoptimin e teknologjive të reja, të cilat kanë pasur një ndikim të drejtpërdrejtë në rritjen e gatishmërisë dhe efikasitetit të ekipeve[3]. Pjesëmarrja në ushtrimin ndërkombëtar "*NATO Cyber Coalition*", ka testuar procedurat e reagimit dhe ka rritur gatishmërinë operative, duke u harmonizuar me objektivat për bashkëpunimin me NATO-n dhe organizimin e stërvitjeve kombëtare.[4] Stërvitjet "*Phishing & Ransomware Response: TTX*" të organizuara nga CRDF Global, me mbështetjen e Departamentit Amerikan të Shtetit, kanë simuluar sulme reale, duke zhvilluar aftësi praktike për menaxhimin e krizave dhe duke mbështetur objektivin për trajtimin efektiv të situatave emergjente.[5] Aktiviteti "*Ec-conclic (cod Red)"* ka shtuar një dimension tjetër në përgatitjen e ekipeve, duke u fokusuar në reagimin ndaj incidenteve kritike. Aktiviteti "*Multi-Sector Cybersecurity TTX: Enhancing Cybersecurity in the Balkan Region"* gjatë muajit Nëntor 2024, i mundësuar nga Hack The Box dhe CRDF Global, ka testuar rezistencën e sistemeve në sektorë të ndryshëm, duke identifikuar pikat e dobëta dhe duke mbështetur objektivin për skanime të vulnerabiliteteve dhe teste të depërtimit në infrastrukturën kritike.[6]

- Përgjatë vitit 2024, **Agjencia Kombëtare e Shoqërisë së Informacionit** ka punuar mbi rezultatet e parashikuara në PBA, duke përmbushur objektivat e paraqitura. Në kuadër të certifikimeve me ISO 27001, ISO 20000-1, ISO 9001, ISO 37001 dhe EIDAS janë rishikuar dhe përmirësuar procedurat për funksionimin e CSIRT qeveritar si dhe është realizuar miratimi dhe përditësimi i procedurave për trajtimin dhe menaxhimin e incidenteve kibernetike. Këto standarde përgjatë vitit 2024, janë audituar nga një entitet ndërkombëtar duke rezultuar në vijimësinë e certifikimeve. Në këtë prizëm, është adaptuar dhe harmonizuar modeli SIM3 për maturitetin e menaxhimit të incidenteve të sigurisë në Drejtorinë e Monitorimit dhe Mbrojtjes Kibernetike për Infrastrukturat e-Gov pranë Agjencisë Kombëtare të Shoqërisë së Informacionit. Si rrjedhojë, CSIRT Qeveritar, është akreditуar si ekip nga bordi i *Trusted Introducer*.

[2] Referuar *Analizimi i infrastrukturave kritike dhe të rëndësishme të informacionit për vlerësimin e menaxhimin e riskut në to.*
[3] Referuar: *Përdorimi i mjeteve teknologjike të Qendrës Kombëtare Operacionale (SOC) për identifikimin, parandalimin,dhe menaxhimin e incidenteve kibernetike.*
[4] Referuar: *Përmbushja e angazhimeve të marra si vend i Aleancës së Atlantikut të Veriut, për hapësirën kibernetike.*
[5] Referuar: *Organizimi i Table Top Exercise për strukturat vendimmarrëse të nivelit të lartë për komunikimin dhe menaxhimin e krizës kibernetike, bazuar edhe në metodologjinë e menaxhimit të krizës kibernetike.*
[6] Referuar: *Testimi i sigurise se sistemeve dhe aplikacioneve ne administrimin e AKSK.*

Gjithashtu, përgjatë këtij viti NAIS G-CSIRT shprehu interesin për përfshirjen në Forumin Ndërkombëtar të Ekipeve të Sigurisë dhe Reagimit ndaj Incidenteve *FIRST*. Mbi këtë është audituar me sukses nga dy entitete (një vendas dhe një i huaj) dhe është në pritje të pranimit në këtë forum. Për sa i përket aspektit teknologjik, është bërë i mundur optimizimi i infrastrukturave të sigurisë dhe zgjerimi i kapaciteteve të mbulimit nëpërmjet zgjidhjeve të ndryshme *hardware* dhe *software* duke iu përgjigjur rezultateve. Gjithashtu, është vazhduar me partneritetin me Microsoft në kuadër të marrëveshjes qeveritare si suport për sigurinë dhe avancimit në arkitekturën *Zero Trust*.

Në terma teknikë, përgjatë vitit 2024, janë zhvilluar skanime aktive për dobësi dhe *penetration test* për infrastrukturat qeveritare duke forcuar nivelin aktual të sigurisë. Gjithashtu, është shtuar përdorimi i inteligjencës artificiale në dhënien e shërbimeve publike të sigurta në kuadër të marrëveshjes qeveritare me Microsoft.

Përgjatë vitit 2024 CSIRT qeveritar ka qenë i ftuar në disa trajnime dhe stërvitje kibernetike të organizuar nga partnerë duke përmbushur objektivat nën rezultatet në lidhje me trajnimet. Madje, janë zhvilluar trajnime të brendshme për stafin mbi sigurinë kibernetike dhe testuar njohuritë me anë të simulimeve të ndryshme të sulmeve *phishing*.

- **Policia e Shtetit** lidhur me zbatimin e Strategjisë Kombëtare për Sigurinë Kibernetike dhe Planin e Veprimit 2024 të dakordësuar, kanë realizuar aktivitete të rëndësishme për forcimin e sigurisë kibernetike dhe luftën kundër krimeve në internet. Një ndër arritjet kryesore ka qenë forcimi i bashkëpunimit me Autoritetin Kombëtar për Sigurisë Kibernetike dhe organizata jo fitimprurëse si iSIGURT.al, për të rritur sigurinë e të miturve në internet. Këto bashkëpunime kanë përfshirë gjithashtu shkëmbimin e informacionit me Agjencinë e Inteligjencës Financiare, për të parandaluar mashtrimet ndërkombëtare dhe për të luftuar krimin financiar që lidhet me transaksionet ndërkombëtare.

  Në fushën e trajnimeve, gjatë vitit 2024 janë zhvilluar shumë aktivitete, për të cilat është mbështetur nga partnerë ndërkombëtarë. Pjesëmarrësit kanë marrë trajnime të specializuara për hetimin e krimeve kibernetike dhe përdorimin e teknologjive të reja, si dronët dhe kriptomonedhat. Specialistët e Policisë së Shtetit kanë marrë pjesë gjithashtu në seminare dhe workshop-e, përfshirë ato në vende si Hungaria, Japonia dhe Austria. Një aktivitet shumë i rëndësishëm ka qenë organizimi i seminarit ndërkombëtar në Tiranë më 25 qershor 2024, me temën "Forcimi i bashkëpunimit dhe shkëmbimi i informacionit në kohë reale ndërmjet LEA-ve dhe CERT-ve". Seminari u mbështet nga Projekti *CyberSEE* dhe pati pjesëmarrës nga EUROPOL, agjencitë LEA dhe CERT të vendeve të Ballkanit Perëndimor, Ukrainës dhe Francës. Ai shërbeu për ndarjen e përvojave ndërkombëtare dhe për krijimin e lidhjeve më të ngushta mes institucioneve të sigurisë kibernetike.

Në fund të vitit 2024, u zhvillua një aktivitet tjetër i rëndësishëm nga 2 deri më 6 dhjetor në Tiranë, ku u realizua një trajnim që fokusohej në bashkëpunimin ndërmjet institucioneve për reagimin ndaj krizave kibernetike. Aktiviteti kishte si qëllim forcimin e aftësive për hetime të përbashkëta dhe shkëmbimin e informacionit për të përballuar kërcënimet kibernetike në rajon dhe më gjerë. Bashkëpunimi ka qenë thelbësor, dhe partnerët në nivel kombëtar dhe ndërkombëtar kanë luajtur një rol kyc në ndihmën që ofrojnë për të adresuar kërcënimet kibernetike.

- **Qendra për Koordinimin Kundër Ekstremizmit të Dhunshëm**, gjatë vitit 2024, ka qenë e angazhuar në një sërë aktivitetesh, ku një ndër iniciativat më të rëndësishme ka qenë trajnimi dhe certifikimi i 220 oficerëve të sigurisë në shkolla, të cilët janë përgatitur për të adresuar çështjet e krimit kibernetik, gjuhës së urrejtjes dhe parandalimin e radikalizmit në ambientet arsimore. Në vijim të kësaj, një bashkëpunim i suksesshëm me OSBE ka mundësuar zhvillimin e një trajnimi dy-ditor për edukimin mediatik dhe informativ, duke ndihmuar pjesëmarrësit të kuptojnë sfidat e dezinformimit dhe rolin e tyre në parandalimin e ekstremizmit të dhunshëm.

  Një tjetër angazhim i rëndësishëm ka qenë fuqizimi i komuniteteve përmes gjashtë takimeve lokale në Kurbin, Kashar, Fier, Vlorë, Kukës dhe Kavajë, ku u krijua një hapësirë bashkëpunimi mes shoqërisë civile, përfaqësuesve fetarë dhe institucioneve arsimore, duke ndihmuar në rritjen e qëndrueshmërisë ndaj formave të ekstremizmit të dhunshëm.

  Në kuadër të promovimit të mesazheve pozitive, QKEDH ka bashkëpunuar me organizatën SHIS për realizimin e 8 videove të shkurtra për rrjetet sociale *(short-reels)*, të cilat synonin të kundërshtojnë narrativat ekstremiste dhe të rrisin ndërgjegjësimin e të rinjve për rreziqet e radikalizmit. Kjo iniciativë u shoqërua edhe me organizimin e një *Bootcamp*-i treditor, ku nxënës të moshave 14-18 vjeç nga 8 shkolla patën mundësinë të diskutojnë dhe të përfshihen në aktivitete edukative mbi ekstremizmin e dhunshëm dhe rolin e tyre si qytetarë aktivë.

  Një tjetër hap përpara ka qenë përpjekja për monitorimin e përmbajtjeve ekstremiste në platformat *online*, një nismë inovative që ka kombinuar analizën e 14 sinjalizuesve të besuar me përdorimin e mjeteve teknologjike për të identifikuar dhe adresuar përmbajtjet problematike. Pavarësisht sfidave, QKEDH ka vijuar përpjekjet e saj në përmbushjen e detyrimeve duke krijuar ura bashkëpunimi mes institucioneve, shoqërisë civile dhe komuniteteve lokale për të adresuar ekstremizmin e dhunshëm dhe për të promovuar një qasje të qëndrueshme në këtë fushë.[7]

[7] Referuar: *Monitorimi dhe parandalimi i fenomeneve, që nxisin ekstremizmin e dhunshëm dhe radikalizimin në shtresat vulnerabël në hapësirën kibernetike.*

B. QËLLIMI I POLITIKËS 2

Ndërtimi i një mjedisi të sigurt kibernetik duke edukuar dhe ndërgjegjësuar shoqërinë në ngritjen e kapaciteteve profesionale në fushën e sigurisë së informacionit.

Objektivat e politikës fokusohen në:

- Rritjen e kapaciteteve profesionale në fushën e sigurisë së informacionit nëpërmjet rishikimit të kurrikulave arsimore;
- Rritjen e ndërgjegjësimit dhe e aftësive profesionale të institucioneve publike dhe private për sigurinë kibernetike;
- Rritjen e ndërgjegjësimit të shoqërisë, për sigurinë kibernetike dhe kërcënimet kibernetike.

Gjatë vitit 2024, Plani i Veprimit i dakordësuar për Politikën 2[8] parashikon zbatimin e gjithsej 8 masave. Nga të cilat:

- 37.5 % e Masave janë realizuar plotësisht;
- 37.5 % e Masave janë realizuar pjesërisht;
- 25 % e Masave nuk ka informacion.

Grafiku 3. Realizimi i masave për Politikën 2

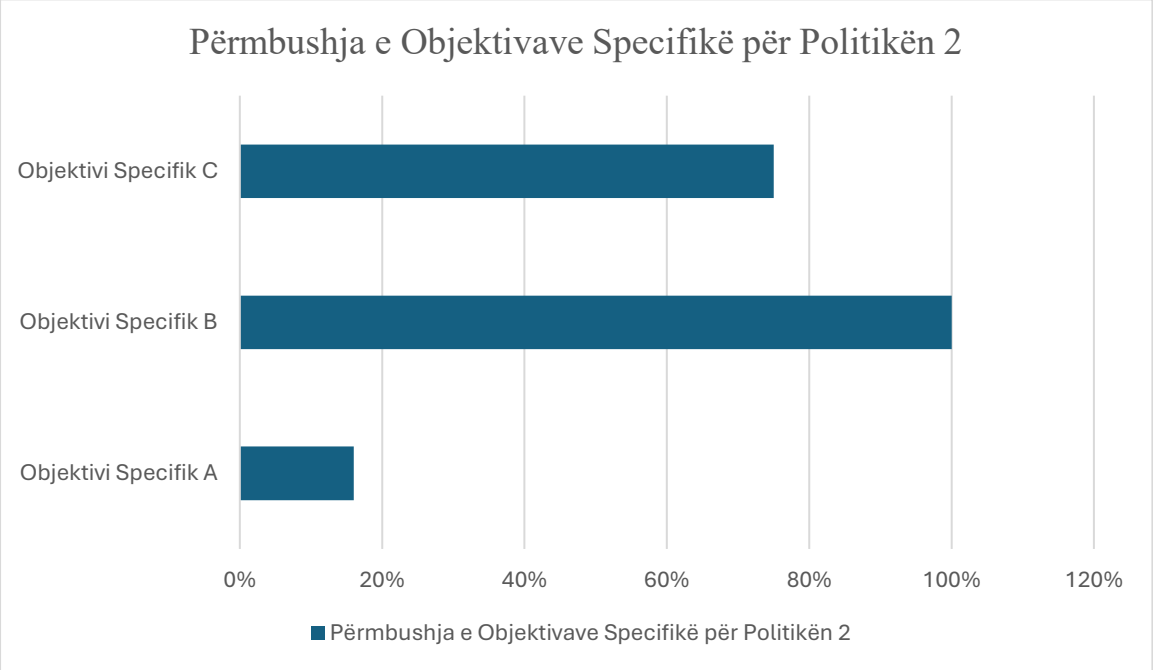
[8] Politika 2. *Ndërtimi i një mjedisi të sigurt kibernetik duke edukuar dhe ndërgjegjësuar shoqërinë në ngritjen e kapaciteteve profesionale në fushën e sigurisë së informacionit.*

Për sa i përket përmbushjes së Objektivave Specifikë të kësaj Politike:

- **Objektivi Specifik A**: Rritja e kapaciteteve profesionale në fushën e sigurisë së informacionit nëpërmjet rishikimit të kurrikulave arsimore
- **Objektivi Specifik B**: Rritja e ndërgjegjësimit dhe e aftësive profesionale të institucioneve publike dhe private për sigurinë kibernetike.
- **Objektivi Specifik C**: Rritje e ndërgjegjësimit të shoqërisë, për sigurinë kibernetike dhe kërcënimet kibernetike.

është vlerësuar se:

- Objektivi Specifik A është realizuar në masën 16 %;
- Objektivi Specifik B është realizuar në masën 100 %;
- Objektivi Specifik C është realizuar në masën 75 %;



Grafiku 4. Përmbushja e Objektivave Specifikë për Politikën 2

Në tërësi, shkalla e zbatimit të Politikës 1 për periudhën raportuese 1 Janar 2024- 31 Dhjetor 2024 është vlerësuar në 75.8 %, bazuar në ecurinë e masave të ndërmarra.

INFORMACION MBI ZBATIMIN E MASAVE:

- **Autoriteti Kombëtar për Sigurinë Kibernetike** ka qenë institucioni drejtues për zbatimin e Politikës 2, duke mbuluar një gamë të gjerë masash që variojnë nga zhvillimi

i trajnimeve praktike deri te ndërgjegjësimi i publikut dhe koordinimi ndërinstitucional. Gjatë vitit 2024, AKSK ka demonstruar një qasje të integruar për përmbushjen e objektivave të strategjisë, në bashkëpunim me institucione kombëtare dhe partnerë ndërkombëtarë. AKSK ka realizuar rreth 10 trajnime në qytete të ndryshme të vendit me fokus në higjienën kibernetike dhe praktikat më mira të sigurisë *online*. Trajnimet kanë qenë në format hibrid dhe janë zhvilluar në bashkëpunim me CRDF Global dhe Departamentin Amerikan të Shtetit, duke përfshirë mbi 500 pjesëmarrës për çdo sesion[9]. Janë hartuar materiale ndërgjegjësuese dhe rekomandime për bizneset[10], si dhe janë organizuar 24 trajnime të dedikuara për operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit. Në partneritet me AKSHI, AKSK ka zhvilluar module trajnimi për CSIRT-et dhe ka organizuar stërvitje në nivel kombëtar, duke përfshirë simulime të avancuara *live-fire* për vlerësimin e gatishmërisë ndaj incidenteve kibernetike[11]. AKSK ka organizuar fushata kombëtare ndërgjegjësimi përmes materialeve edukative dhe webinareve[12]. Është krijuar një seksion i dedikuar në website-in e Autoritetit, që përfshin përmbajtje të strukturuar sipas tematikave mujore[13]. Në bashkëpunim me institucione të tjera, ka nisur puna për hartimin e një udhëzimi për procedurat e ndarjes dhe shpërndarjes së informacionit[14].

- **Agjencia Kombëtare për Shoqërinë e Informacionit** ka kontribuar si një aktor i rëndësishëm në rritjen e kapaciteteve teknike dhe menaxheriale në nivel qendror, në përputhje me zbatueshmërinë e masave operacionale. Ajo ka luajtur një rol të rëndësishëm në konsolidimin e kapaciteteve të CSIRT-it qeveritar dhe në ndërtimin e një arkitekturë të qëndrueshme mbrojtëse për sistemet dhe të dhënat publike. AKSHI ka kontribuar ndjeshëm në forcimin e kapaciteteve institucionale në fushën e sigurisë kibernetike, në përputhje me objektivat e Strategjisë Kombëtare.

  Gjatë vitit 2024, në bashkëpunim me AKSK, janë zhvilluar trajnime të specializuara për anëtarët e ekipeve CSIRT dhe drejtuesit e nivelit ekzekutiv të institucioneve shtetërore[15]. Këto trajnime janë organizuar si në format fizik, ashtu edhe *online*, me qëllim për të rritur ndërgjegjësimin strategjik dhe përgjegjësinë institucionale ndaj kërcënimeve digjitale. AKSHI ka drejtuar gjithashtu organizimin e disa stërvitjeve kombëtare me skenarë teknikë dhe operacionalë, duke testuar aftësinë reaguese të institucioneve publike përballë sulmeve kibernetike[16]. Një komponent i rëndësishëm i këtij angazhimi ka qenë përmirësimi dhe harmonizimi i proceseve të brendshme të

[9] Referuar: *Trajnime periodike, për thellimin e njohurive në sigurinë kibernetike, sipas dinamikës së fushës, për stafin administrativ në nivel qendror dhe në nivel lokal*
[10] Referuar: *Hartimi i materialeve udhëzuese, ndërgjegjësuese dhe rekomanduese për biznesin*
[11] Referuar: *Rritja e kapaciteteve të CSIRT-eve në nivel kombëtar dhe nivelit ekzekutiv të administratës publike nëpërmjet trajnimeve dhe stërvitjeve kibernetike*
[12] Referuar: *Rritja e ndërgjegjësimit të shoqërisë për sigurinë kibernetike, duke përdorur hapësirat e duhura për realizimin e tyre, përfshirë edhe mediat audiovizive apo edhe ato sociale*
[13] Referuar: *Krijimi i një seksioni në webfaqen e AKSK, për të ndarë materiale edukative me qëllimi ndërgjegjësimin mbi reziqet dhe sigurinë në internet; Fushata ndërgjegjësimi të implementuara përmes platformës dhe të organizuara sipas temave specifike për çdo muaj; Hartimi i materialeve ndërgjegjësuese të platformës, si udhëzime, këshilla, video demonstruese, quiz-e, etj*
[14] Referuar: *Hartimi i një udhëzimi të përbashkët me institucionet mbi procedurën për ndërveprimin dhe shpërndarjen e informacionit*
[15] Referuar: *Organizimi i trajnimeve në fushën e sigurisë kibernetike për CSIRT-et në nivel kombëtar; Organizimi trajnimeve në fushën e sigurisë kibernetike për nivelin drejtues ekzekutiv të administratës publike*
[16] Referuar: *Organizimi i stërvitjeve kibernetike në nivel kombëtar*

CSIRT-it qeveritar sipas standardeve ndërkombëtare ISO 27001, ISO 20000-1 dhe EIDAS, duke mundësuar marrjen e akreditimit nga Trusted Introducer, një njohje që e vendos Shqipërinë në nivelin e ekipeve të besuara të reagimit në Evropë.

Në aspektin teknik, AKSHI ka realizuar skanime aktive për zbulimin e dobësive në sistemet kritike qeveritare dhe ka implementuar teste penetrimi për të vlerësuar sigurinë reale të infrastrukturave publike[17]. Kjo është shoqëruar me investime në teknologji të avancuar, si arkitektura *"Zero Trust"* dhe përdorimi i inteligjencës artificiale për ofrimin e shërbimeve më të sigurta dhe të personalizuara për qytetarët. Për më tepër, AKSHI ka kontribuar në hartimin e një udhëzimi të përbashkët me institucione të tjera për përmirësimin e procedurave të ndarjes së informacionit dhe koordinimit ndërinstitucional[18], duke rritur efektivitetin në menaxhimin e informacionit të ndjeshëm dhe ndërtimin e një qasjeje të unifikuar ndaj incidenteve kibernetike.

- **Ministria e Arsimit dhe Sportit** ka luajtur një rol aktiv në përfshirjen e komponentëve të sigurisë kibernetike në sistemin arsimor dhe në forcimin e kapaciteteve edukative për mbrojtjen digjitale të fëmijëve dhe të rinjve. Kontributi i saj ka qenë thelbësor për të siguruar që çështjet e sigurisë *online* të bëhen pjesë përbërëse e arsimit në Shqipëri.
  MAS ka shfaqur një angazhim të qëndrueshëm në përfshirjen e tematikës së sigurisë kibernetike në sistemin arsimor shqiptar. Përmes një programi të gjerë trajnimesh, janë përgatitur mbi 400 mësues të arsimit fillor dhe të mesëm për të përdorur teknologjinë në mënyrë të sigurt në procesin mësimor[19]. Janë trajnuar gjithashtu mbi 200 drejtues të shkollave në menaxhimin e mjediseve arsimore përmes platformave digjitale dhe mjeteve të reja të sigurisë. MAS ka hartuar dhe zbatuar udhëzime dhe rregullore për mbrojtjen e të dhënave të nxënësve, si dhe ka ngritur një platformë për monitorimin e aktivitetit *online* në shkolla. Në bashkëpunim me AKSK, vijon puna për hartimin e rekomandimeve për përfshirjen e temave të internetit të sigurt në kurrikulat universitare[20], duke kontribuar kështu në edukimin e qëndrueshëm të brezave të rinj.

- **Policia e Shtetit** ka kontribuar në fuqizimin e përgjigjes kombëtare ndaj krimeve kibernetike dhe ka rritur bashkëpunimin ndërkombëtar për mbrojtjen e të drejtave digjitale të qytetarëve. Në fokus të veçantë ka qenë mbrojtja e të miturve dhe lufta kundër abuzimeve *online* përmes koordinimit me institucionet publike dhe platformat ndërkombëtare. Policia e Shtetit ka shfaqur një rol të rëndësishëm në ndërveprimin institucional për sigurinë kibernetike dhe mbrojtjen e qytetarëve në hapësirën digjitale. Përmes bashkëpunimit me AKSK dhe platformën iSigurt.al, janë realizuar fushata për mbrojtjen e të miturve *online* dhe edukimin e tyre mbi rreziqet në rrjet[21].

[17] Referuar: *Hartimi i materialeve ndërgjegjësuese të platformës, si udhëzime, këshilla, video demonstruese, quiz-e, etj.*
[18] Referuar: *Hartimi i një udhëzimi të përbashkët me institucionet mbi procedurën për ndërveprimin dhe shpërndarjen e informacionit*
[19] Referuar: *Hartimi i materialeve ndërgjegjësuese dhe edukative, kurse e-learning dhe aktivitete të tjera trajnimi për të rinjtë*
[20] Referuar: *Hartimi i rekomandimeve për integrimin në kurrikula universitare të informacioneve në lidhje me Internetin e Sigurtë*
[21] Referuar*: Krijimin e një platforme edukative online, për sigurinë kibernetike, për të rritur ndërgjegjësimin në grupmosha të ndryshme të shoqërisë, për përdorimin e Internetit të sigurt dhe të infrastrukturës digjitale*

PSH ka krijuar ura bashkëpunimi me kompani ndërkombëtare si Meta, TikTok dhe Google për mbylljen e adresave të rrezikshme dhe për trajtimin e ankesave të qytetarëve për abuzime në rrjetet sociale. Janë realizuar trajnime të specializuara të stafit të tyre dhe janë zhvilluar takime me përfaqësues të platformave për forcimin e bashkëpunimit ndërkombëtar në luftën kundër krimeve digjitale. Gjithashtu, PSH ka marrë pjesë në projektet e monitorimit të aktiviteteve në *dark web* dhe ka zhvilluar fushata për parandalimin e mashtrimeve digjitale dhe pastrimit të parave *online*, duke forcuar kështu komponentin hetimor dhe reagues ndaj rreziqeve hibride.

- **Agjencia Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijës** ka dhënë mbështetje të vazhdueshme për të promovuar një mjedis digjital të sigurt për fëmijët. Në bashkëpunim me AKSK, ajo ka ndërmarrë një sërë iniciativash për ndërgjegjësimin dhe edukimin e fëmijëve, prindërve dhe profesionistëve mbi rreziqet në internet dhe masat për mbrojtjen e të miturve. Gjatë vitit 2024, janë realizuar mbi 30 aktivitete ndërgjegjësuese në shkolla 9-vjeçare dhe të mesme në disa qytete të vendit, si dhe janë organizuar 4 workshop-e për prindër dhe profesionistë në Tiranë, Durrës, Kukës dhe Cërrik, duke arritur një audiencë mbi 1300 fëmijë dhe qindra të rritur[22].

  Janë hartuar mekanizma për raportimin e rasteve të bullizmit, ngacmimeve dhe abuzimeve online, si dhe janë krijuar protokolle bashkëpunimi me Policinë e Shtetit dhe AKSK për mbylljen e faqeve dhe identifikimin e autorëve. Janë trajtuar raste të keqpërdorimit të të dhënave të fëmijëve në rrjet, duke përfshirë edhe ofrimin e ndihmës psikologjike dhe mbështetjes sociale për fëmijët e prekur. ASHDMF ka kontribuar gjithashtu në edukimin e prindërve dhe punonjësve të shërbimeve sociale për të forcuar sigurinë në komunitet dhe për të parandaluar dhunën digjitale në mjediset arsimore.

C. QËLLIMI I POLITIKËS 3

Krijimi i mekanizmave të nevojshëm për sigurinë e fëmijëve në hapësirën kibernetike, duke përgatitur njëkohësisht brezin e ri të aftë për të përfituar nga përparësitë e teknologjisë së informacionit dhe për të përballuar sfidat e zhvillimit.

Objektivat e politikës fokusohen në:

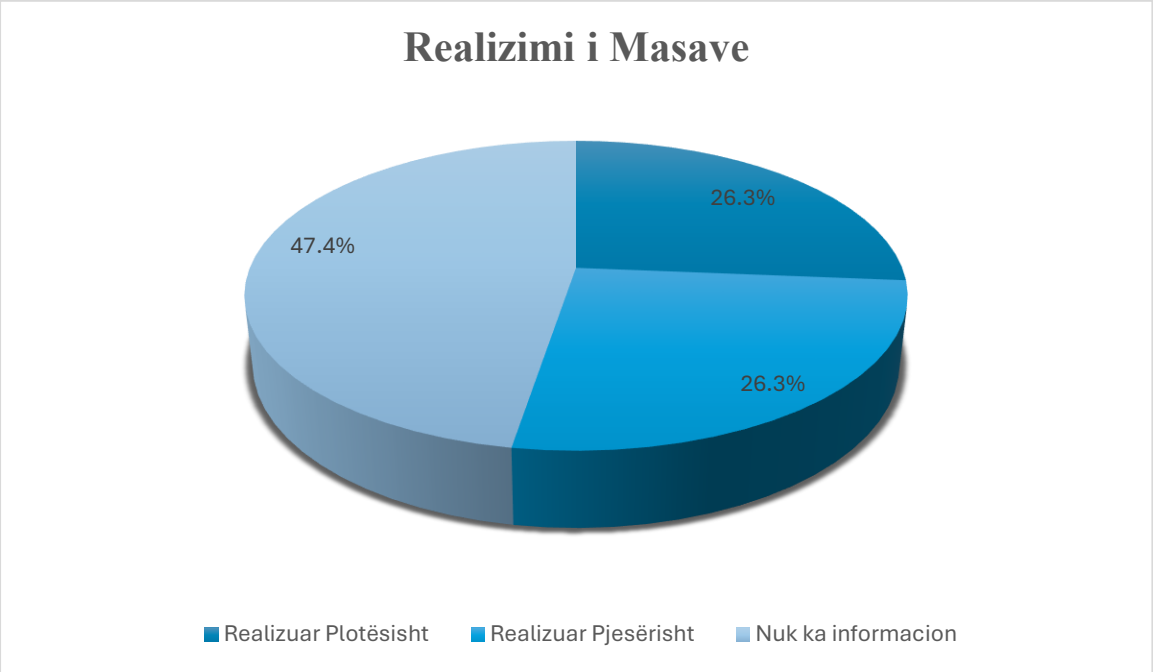
- Forcimi i kuadrit ligjor për rritjen e sigurisë së fëmijëve në Internet;
- Parandalimi i abuzimit seksual të fëmijëve në Internet nëpërmjet rritjes së ndërgjëgjësimit dhe krijimit të hapësirave të sigurta për lundrimin në Internet;
- Hetimi efektiv dhe sjellja para drejtësisë e autorëve të krimeve kibernetike ndaj fëmijëve, me fokus abuzimin dhe shfrytëzimin seksual;

[22] Referuar*: Krijimin e një platforme edukative online, për sigurinë kibernetike, për të rritur ndërgjegjësimin në grupmosha të ndryshme të shoqërisë, për përdorimin e Internetit të sigurt dhe të infrastrukturës digjitale*

- Rritja e ndërgjegjësimit dhe edukimi tek të gjitha segmentet e shoqërisë për përdorimin e sigurtë të Internetit nga fëmijët;
- Forcimi i bashkëpunimit ndërsektorial për mbrojtjen e fëmijëve në Internet.

Gjatë vitit 2024, Plani i Veprimit i dakordësuar për Politikën 3 parashikon zbatimin e gjithsej 19 masave. Nga të cilat:

- 26.3 % e Masave janë realizuar plotësisht;
- 26.3 % e Masave janë realizuar pjesërisht;
- 47.4 % e Masave nuk ka informacion.



Grafiku 5. Realizimi i Masave të Politikës 3

Për sa i përket përmbushjes së Objektivave Specifikë të kësaj Politike:

- **Objektivi Specifik A:** Forcimi i kuadrit ligjor për rritjen e sigurisë së fëmijëve në Internet.

- **Objektivi Specifik B**: Parandalimi i abuzimit seksual të fëmijëve në Internet nëpërmjet rritjes së ndërgjëgjësimit dhe krijimit të hapësirave të sigurta për lundrimin në Internet.

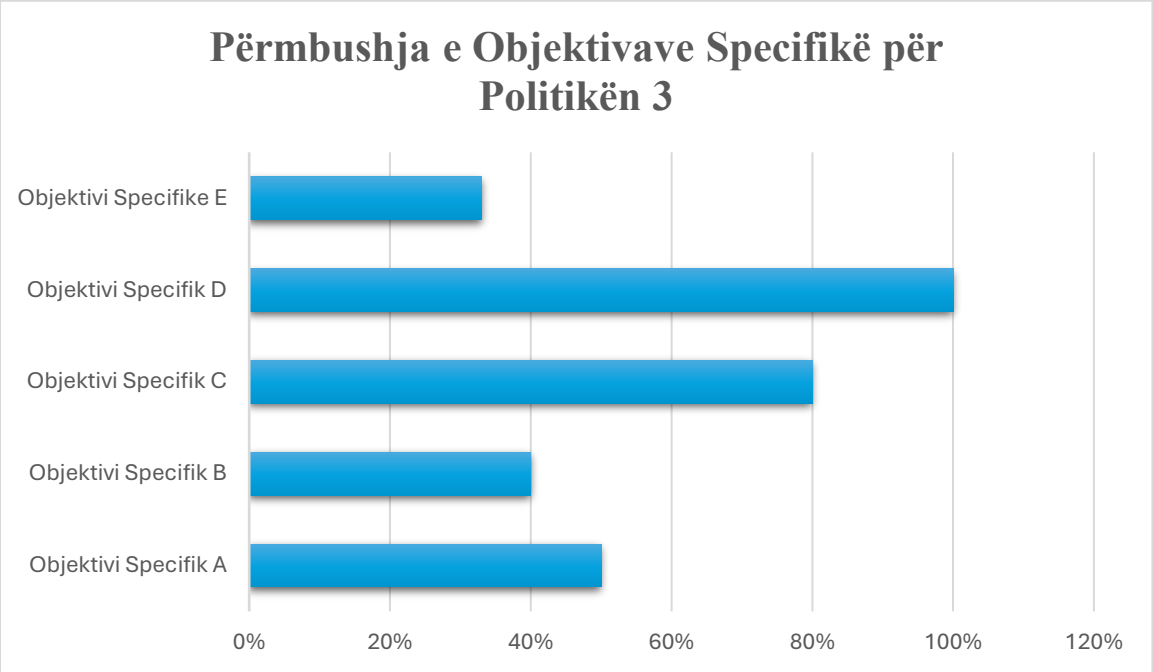
- **Objektivi Specifik C**: Hetimi efektiv dhe sjellja para drejtësisë e autorëve të krimeve kibernetike ndaj fëmijëve, me fokus abuzimin dhe shfrytëzimin seksual.

- **Objektivi Specifik D**: Rritja e ndërgjegjësimit dhe edukimi tek të gjitha segmentet e shoqërisë për përdorimin e sigurtë të Internetit nga fëmijët.

- **Objektivi Specifik E**: Forcimi i bashkëpunimit ndërsektorial për mbrojtjen e fëmijëve në Internet.

është vlerësuar se:

- Objektivi Specifik A është realizuar në masën 50 %;
- Objektivi Specifik B është realizuar në masën 40 %;
- Objektivi Specifik C është realizuar në masën 80 %;
- Objektivi Specifik D është realizuar në masën 100 %;
- Objektivi Specifik E është realizuar në masën 33 %.



Grafiku 6. Përmbushja e Objektivave Specifikë për Politikën 3

Në tërësi, shkalla e zbatimit të Politikës 3 për periudhën raportuese 1 Janar 2024 - 31 Dhjetor 2024 është vlerësuar në 38 %, bazuar në ecurinë e masave të ndërmarra.

INFORMACION MBI ZBATIMIN E MASAVE:

- **Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK)** gjatë vitit 2024 ka zhvilluar me sukses trajnime dhe aktivitete sensibilizuese në fushën e mbrojtjes së fëmijëve dhe të rinjve nga kërcënimet kibernetike, duke ndërmarrë një sërë iniciativash, të cilat kanë rritur kapacitetet në fushën e sigurisë kibernetike dhe kanë forcuar bashkëpunimin me institucionet përgjegjëse për mbrojtjen e fëmijëve dhe të rinjve.

Në Shkurt të vitit 2024, AKSK dhe ASHDMF nënshkruan një marrëveshje bashkëpunimi me qëllim forcimin e ndërgjegjësimit dhe edukimit të fëmijëve e të rinjve në fushën e sigurisë në internet. Në zbatim të saj, u realizuan një sërë aktivitetesh, përfshirë konferencën kushtuar Ditës Ndërkombëtare të Internetit të Sigurt, një tryezë të rrumbullakët me përfaqësues të institucioneve kryesore dhe një fushatë të gjerë ndërgjegjësimi në shkollat e vendit. Gjatë vitit 2024 u realizuan gjithsej 37 aktivitete në shkolla, ku u përfshinë 174 oficerë sigurie dhe 423 mësues në trajnime, si dhe u organizuan gjithashtu *webinare* me një numër të konsiderueshëm pjesëmarrësish.

Gjithashtu, në Dhjetor 2024 u lidh një marrëveshje bashkëpunimi edhe me Qendrën për Mbrojtjen e të Drejtave të Fëmijëve në Shqipëri, duke zgjeruar rrjetin e partnerëve të angazhuar në këtë mision. Përmes platformës "Raporto", janë trajtuar 224 raste të raportuara lidhur me sigurinë *online* të fëmijëve, duke u ndjekur në bashkëpunim me institucionet përgjegjëse. AKSK, në bashkëpunim me UNICEF dhe institucione të tjera partnere, ka theksuar rëndësinë e masave të përbashkëta për të adresuar rreziqet në rritje që lidhen me aplikacionet dhe përmbajtjet e dëmshme në internet.

Një tjetër nismë me rëndësi të veçantë ishte organizimi i një tryeze të përbashkët ndërinstitucionale më datë 30 Prill 2024, e cila kishte në fokus adresimin e problematikave që lidhen me sigurinë e fëmijëve në internet. Si rezultat i diskutimeve, iu drejtua një shkresë Ministrisë së Drejtësisë me propozimin për të ndërmarrë masa ligjore që përfshijnë kriminalizimin e bullizmit *online*. Kjo tryezë, me pjesëmarrjen e të gjithë aktorëve përkatës, u pasua edhe në muajin 18 Nëntor 2024, me qëllim forcimin e ndërgjegjësimit dhe thellimin e angazhimit institucional ndaj kësaj çështjeje.

- **Ministria e Arsimit dhe Sportit** ka realizuar një sërë iniciativash të rëndësishme bazuar në raportimin lidhur me procesin e zbatimit të masave të parashikuara në Planin e Veprimit të dakordësuar për vitin 2024, të "Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025", duke përfshirë aktivitete dhe projekte që kanë ndikuar në përmirësimin e cilësisë së arsimit dhe në forcimin e sistemeve të sigurisë për nxënësit dhe studentët.
  Lidhur me sigurinë kibernetike të nxënësve dhe mbrojtjen e tyre nga përmbajtje të paligjshme dhe të dëmshme në institucionet arsimore parauniversitare janë në zbatim aktet e mëposhtme:
  a. Udhëzimi i përbashkët midis Ministrisë së Arsimit, Sportit dhe Rinisë (MARS, sot MAS) dhe Ministrisë së Shëndetësisë dhe Mbrojtjes Sociale (MSHMS) Nr. 658, datë 23.09.2019, "*Për procedurat dhe veprimet që ndërmarrin strukturat arsimore, në bashkëpunim me strukturat e mbrojtjes së fëmijëve, në rastet kur në mjediset e institucionit arsimor parauniversitar konstatohet se një fëmijë është duke aksesuar në internet përmbajtje të paligjshme dhe/ose të dëmshme për moshën e tij*"[23].

[23] https://csl.edu.al/wp-content/uploads/2021/10/Udh%C3%ABzim-i-p%C3%ABrbashk%C3%ABt-nr.-658-dat%C3%AB-23.9.2019.pdf

b. Udhëzimi Nr. 34, datë 16.11.2018 *"Për ndalimin e telefonit celular në institucionet arsimore parauniversitare, si dhe nga mësuesi ashtu dhe nga nxënësi"*[24].
c. Urdhri Nr. 493, datë 30.07.2018 *"Për mospërdorimin e telefonit celular gjatë procesit mësimor në shkolla".*

Në shkolla është krijuar një rrjet bashkëpunimi me prindërit dhe njësitë e mbrojtjes së fëmijëve (NJMF), me qëllim mbrojtjen e të miturve nga dhuna kibernetike. Gjithashtu, janë zhvilluar bashkëpunime të tjera me aktorë lokalë për forcimin e masave parandaluese ndaj trafikimit të qenieve njerëzore, si dhe për adresimin e rasteve të bullizmit dhe ekstremizmit të dhunshëm. Raportimi javor nga oficerët e sigurisë në shkolla është realizuar në mënyrë të vazhduar, me qëllim rritjen e ndërgjegjësimit dhe trajtimin e rasteve të bullizmit dhe abuzimit *online,* duke përfshirë në këtë proces mësuesit, nxënësit dhe prindërit.

Janë zhvilluar orë informuese dhe sensibilizuese në bashkëpunim me specialistë të Policisë së Shtetit, në lidhje me penalitetet ligjore të personave që kryejnë krime në internet dhe për të prezantuar mekanizmat e raportimit të këtyre krimeve. Gjatë vitit 2024 është hartuar "Raporti i Identifikimit të Parandalimit e Raportimit të Dhunës, Bullizmit dhe forma të tjera të IAP", për vitin shkollor 2023-2024. Në funksion të forcimit të mekanizmave të mbrojtjes, Ministria ka intensifikuar bashkëpunimin me institucione shtetërore dhe organizata ndërkombëtare, me qëllim përmirësimin e mbrojtjes së fëmijëve nga përmbajtjet e dëmshme dhe fenomenet negative që qarkullojnë në mjedisin virtual.

- **Agjencia Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijës** (ASHMDF) në bashkëpunim me Autoritetin Kombëtar për Sigurinë Kibernetike (AKSK), ka ndërmarrë një sërë aktivitetesh dhe fushatash ndërgjegjësuese të fokusuara në forcimin e mekanizmave të mbrojtjes së fëmijëve dhe garantimin e sigurisë së tyre në hapësirën digjitale. Këto iniciativa janë zhvilluar në përputhje me objektivat e Strategjisë Kombëtare për Sigurinë Kibernetike, Agjendës Kombëtare për të Drejtat e Fëmijëve, si dhe në zbatim të ligjit Nr. 18/2017 *"Për të Drejtat dhe Mbrojtjen e Fëmijës"*. Veprimtaritë e ndërmarra synojnë të ndërtojnë një qasje të qëndrueshme për mbrojtjen e të miturve ndaj rreziqeve që lidhen me përdorimin e internetit dhe teknologjive të informacionit, duke nxitur ndërgjegjësimin, edukimin dhe përfshirjen e fëmijëve, prindërve dhe komunitetit arsimor.

  Një ndër objektivat kryesorë për vitin 2024 ka qenë rritja e ndërgjegjësimit dhe edukimi i fëmijëve, mësuesve dhe profesionistëve të tjerë mbi përdorimin e sigurt të internetit, me theks të veçantë në mbrojtjen e fëmijëve në mjedisin digjital. Në këtë kuadër, gjatë periudhës Shkurt - Dhjetor 2024, janë organizuar katër *workshop-e* me karakter informues për prindër dhe profesionistë të fushës, me pjesëmarrjen e rreth 200

[24] https://arsimi.gov.al/wp-content/uploads/2018/11/Udhezim-nr-34-dt-16-11-2018-per-ndalin-e-telefonit-celular.pdf

individëve, përfshirë mësues, punonjës psikosocialë dhe specialistë të tjerë në qytetet Tiranë, Kukës, Durrës dhe Cërrik.

Njëkohësisht, janë realizuar 30 aktivitete sensibilizuese në shkollat 9-vjeçare dhe të mesme, ku morën pjesë rreth 1300 fëmijë. Këto aktivitete me karakter edukativ kishin për qëllim nxitjen e sjelljeve të sigurta dhe të përgjegjshme në mjedisin *online.* Aktivitetet ndërgjegjësuese kanë përfshirë trajnime të fokusuara në mënyrat e identifikimit dhe raportimit të rasteve të bullizmit, ngacmimeve dhe kërcënimeve në mjedisin *online*, si dhe prezantimin e praktikave më të mira për lundrim të sigurt dhe të përgjegjshëm në internet. Këto ndërhyrje, përfshirë takimet e zhvilluara në shkollat e Tiranës dhe në qytete të tjera, kanë kontribuar në krijimin e një mjedisi digjital më të sigurt për fëmijët, duke rritur nivelin e ndërgjegjësimit dhe njohurive të prindërve, mësuesve dhe profesionistëve të tjerë mbi sfidat dhe masat e nevojshme për garantimin e sigurisë kibernetike.

Në përputhje me detyrimet e përcaktuara në kuadrin ligjor në fuqi, gjatë vitit 2024, Agjencia Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijës ka realizuar analizën dhe shqyrtimin e rasteve të raportuara që lidhen me keqpërdorimin e të dhënave të fëmijëve në rrjetet sociale. Vëmendje e veçantë i është kushtuar rasteve që përfshijnë krijimin e profileve të rreme dhe shpërndarjen e materialeve denigruese apo bullizuese ndaj fëmijëve. Në funksion të adresimit të këtyre problematikave, janë administruar 61 raportime të ardhura nga fëmijë, prindër dhe punonjës të shërbimeve të mbrojtjes së fëmijës, të cilat kanë sjellë reagime të menjëhershme nga Autoriteti Kombëtar për Sigurinë Kibernetike dhe strukturat përkatëse të Policisë së Shtetit për identifikimin dhe ndjekjen e autorëve si dhe mbylljen e faqeve me përmbajtje të dëmshme.

Gjithashtu, gjatë vitit 2024, është intensifikuar puna për menaxhimin e rasteve të dhunës ndaj fëmijëve në mjedisin digjital, duke përfshirë shantazhe, kërcënime, publikim të materialeve intime (foto/video), krijimin e adresave të rreme dhe raste të bullizmit *online*, të ndodhura kryesisht në platforma të tilla si *WhatsApp*, *TikTok*, *Instagram* dhe rrjete të tjera sociale.

Punonjësit për Mbrojtjen e Fëmijës kanë trajtuar 16 raste të tilla në bashkëpunim të ngushtë me strukturat e policisë dhe njësitë përkatëse të krimit kibernetik, duke siguruar mbylljen e adresave të paligjshme dhe identifikimin e autorëve. Për çdo rast të dhunës digjitale ndaj fëmijëve, janë ofruar shërbime psikologjike, kryesisht në mjediset shkollore dhe në raste të veçanta, nga psikologë të licencuar. Situatat janë vlerësuar nga Punonjësit për Mbrojtjen e Fëmijës (PMF), të cilët kanë hartuar plane individuale të mbrojtjes për çdo fëmijë të prekur dhe kanë realizuar monitorim periodik për të garantuar mbështetje të qëndrueshme dhe mbrojtje nga rreziqet *online*. Ky proces ka pasur një ndikim domethënës në rritjen e ndërgjegjësimit institucional dhe shoqëror mbi rëndësinë e sigurisë së fëmijëve në mjedisin digjital, duke kontribuar ndjeshëm në

parandalimin dhe adresimin e përmbajtjeve të paligjshme dhe të dëmshme ndaj tyre në internet.

- **Policia e Shtetit** përmes strukturave të saj të specializuara, ka realizuar një sërë aktivitetesh të rëndësishme në funksion të forcimit të sigurisë kibernetike dhe luftës kundër krimeve që kryhen përmes internetit. Në këtë kuadër, Drejtoria për Hetimin e Krimeve Kibernetike dhe strukturat e tjera përgjegjëse kanë kontribuar në rritjen e ndërgjegjësimit publik për çështjet e sigurisë në mjedisin digjital. Ndër arritjet më të spikatura përmendet forcimi i bashkëpunimit me Autoritetin Kombëtar për Sigurinë Kibernetike dhe organizata të shoqërisë civile si iSIGURT.al, me qëllim rritjen e nivelit të mbrojtjes së të miturve në internet. Në funksion të forcimit të mekanizmave të parandalimit të mashtrimeve dhe krimeve financiare të lidhura me transaksionet ndërkombëtare, janë intensifikuar shkëmbimet e informacionit dhe bashkëpunimi ndërinstitucional me Agjencinë e Inteligjencës Financiare. Këto shkëmbime synojnë rritjen e kapaciteteve për identifikimin e rasteve të dyshuara dhe garantimin e transparencës në transaksionet ndërkufitare. Një tjetër komponent me rëndësi strategjike ka qenë bashkëpunimi me kompani ndërkombëtare të teknologjisë dhe rrjeteve sociale si *"Meta Platforms Inc."*, *"Google"* dhe *"TikTok"*, me qëllim mbrojtjen e të dhënave personale të qytetarëve dhe luftimin e aktiviteteve të paligjshme në hapësirën digjitale. Në këtë kuadër, janë zhvilluar takime fizike dhe virtuale me përfaqësues të këtyre platformave, me fokus në përmirësimin e mekanizmave të raportimit dhe ndërhyrjes ndaj përmbajtjeve të dëmshme dhe llogarive të falsifikuara.

  Gjithashtu, janë organizuar trajnime të specializuara për stafin e Policisë së Shtetit në drejtim të menaxhimit të rasteve që përfshijnë shkelje të sigurisë në rrjetet sociale dhe mbrojtjen e të drejtave të përdoruesve. Për më tepër është ofruar asistencë dhe mbështetje për qytetarët që janë përballur me problematika të tilla duke mundësuar ndërhyrje konkrete në rastet e cenimit të privatësisë apo përhapjes së përmbajtjeve të dëmshme.

  Në kuadër të "Paketës së Sigurisë në Shkolla", janë zhvilluar aktivitete të rregullta me fokus edukimin e të miturve për përdorimin e sigurt të internetit dhe parandalimin e bullizmit në rrjetet sociale. Takime të tjera janë zhvilluar me përfaqësues të Bashkimit Evropian, me qëllim përfshirjen në projekte ndërkombëtare që synojnë rritjen e kapaciteteve hetimore dhe përmirësimin e shkëmbimit të informacionit. Gjithashtu, është monitoruar në vazhdimësi aktiviteti në tregjet ilegale të *darkweb-it*, duke përfshirë platformat e njohura si Hansa Market dhe Agartha Market, me qëllim identifikimin dhe ndalimin e veprimtarive të paligjshme. Ky bashkëpunim i gjerë ndërinstitucional dhe ndërkombëtar ka qenë thelbësor për adresimin e kërcënimeve kibernetike dhe ka ndihmuar ndjeshëm në ndërtimin e një sistemi më të sigurt për qytetarët dhe institucionet.

D. QËLLIMI I POLITIKËS 4

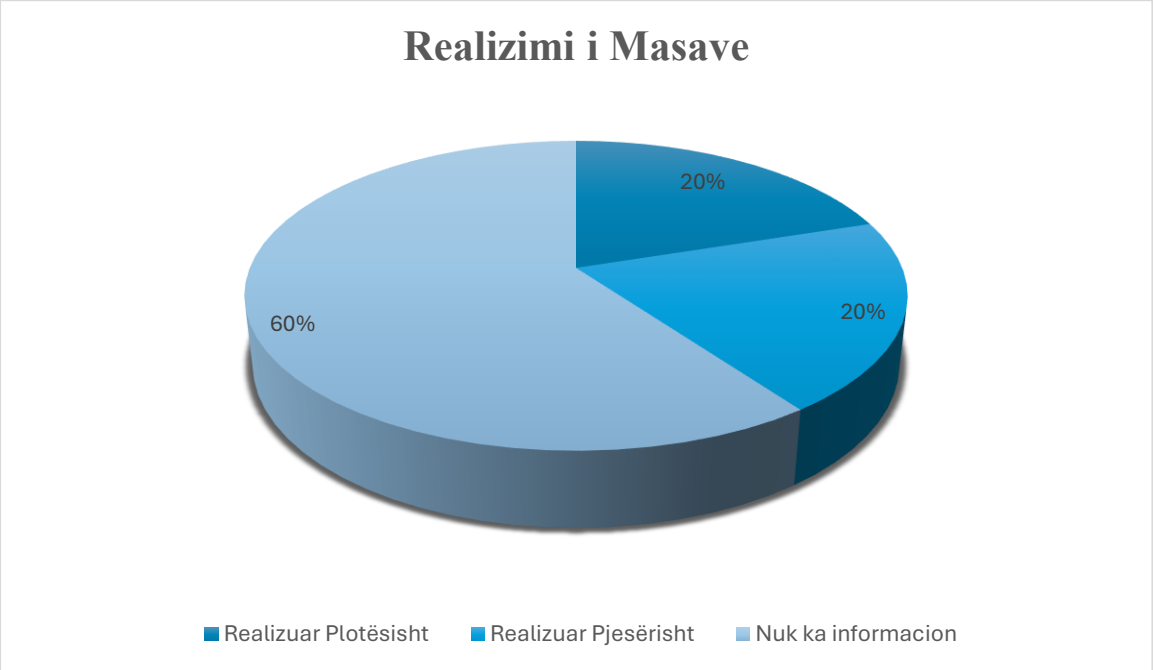
Rritja e bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike me partnerët strategjik.

Objektivat e politikës fokusohen në:

- Forcimi i bashkëpunimit institucional në nivel kombëtar;
- Forcimi i bashkëpunimit ndërkombëtar në fushën e sigurisë dhe mbrojtjes kibernetike dhe luftës kundër ekstremizmit të dhunshëm dhe radikalizimit.

Gjatë vitit 2024, Plani i Veprimit të dakordësuar për Politikën 4 parashikon zbatimin e gjithsej 5 masave. Nga të cilat:

- 20 % e Masave janë realizuar plotësisht;
- 20 % e Masave janë realizuar pjesërisht;
- 60 % e Masave nuk ka informacion.



Grafiku 7. Realizimi i Masave të Politikës 4

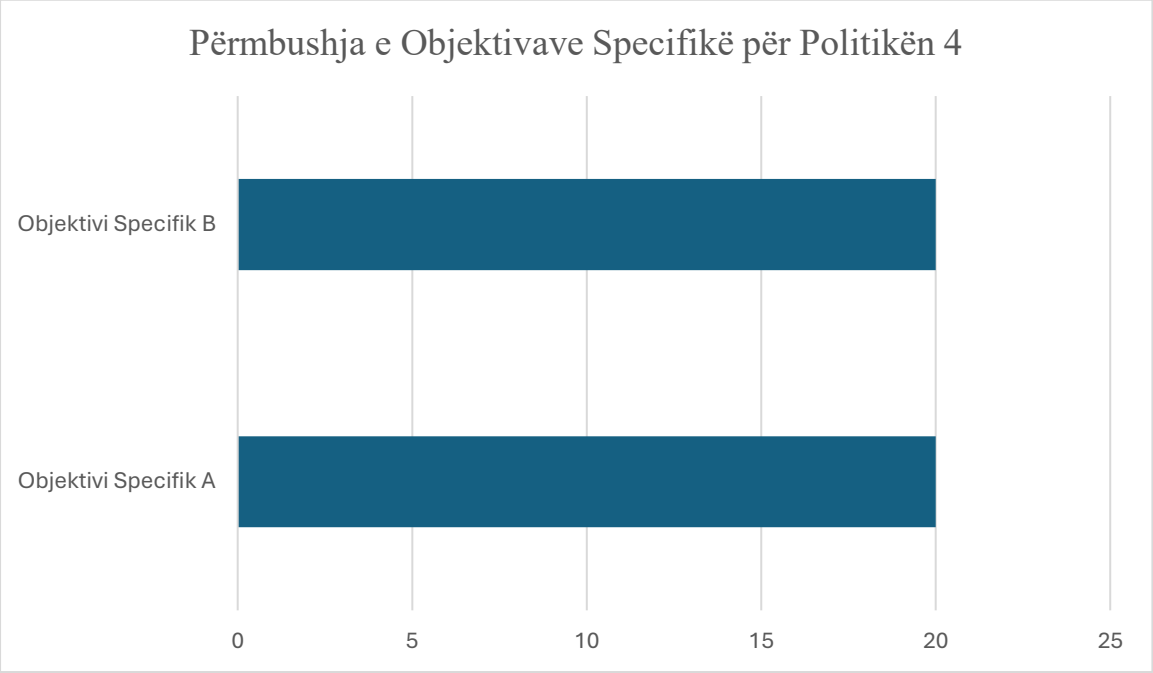
Për sa i përket përmbushjes së Objektivave Specifikë të kësaj Politike:

- **Objektivi Specifik A:** Forcimi i bashkëpunimit institucional në nivel kombëtar.

- **Objektivi Specifik B**: Forcimi i bashkëpunimit ndërkombëtar në fushën e sigurisë dhe mbrojtjes kibernetike dhe luftës kundër ekstremizmit të dhunshëm dhe radikalizimit.

është vlerësuar se:

- Objektivi Specifik A është realizuar në masën 20 %;
- Objektivi Specifik B është realizuar në masën 20 %.



Grafiku 8. Përmbushja e Objektivave Specifikë për Politikën 4

INFORMACION MBI ZBATIMIN E MASAVE:

- **Autoriteti Kombëtar për Sigurinë Kibernetike** (AKSK) ka vijuar punën për forcimin e sigurisë kibernetike në Shqipëri, përmes nënshkrimit të disa marrëveshjeve dhe partneriteteve të rëndësishme me institucione kombëtare dhe ndërkombëtare. Me synimin për të rritur bashkëpunimin në nivel kombëtar dhe për të forcuar mbrojtjen ndaj rreziqeve kibernetike, Autoriteti ka inicuar dhe formalizuar marrëveshje bashkëpunimi me institucione publike dhe private brenda vendit.
  Marrëveshjet e nënshkruara gjatë vitit 2024, janë si më poshtë vijojnë:
  a. Marrëveshje me Presidencën;
  b. Marrëveshje me Autoritetin e Mbikëqyrjes Financiare;
  c. Marrëveshje me Agjencinë Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijëve;
  d. Memorandum Mirëkuptimi me Shoqatën e Bankave;
  e. Marrëveshje me Eurosig;
  f. Marrëveshje me Drejtorinë Kombëtare për Sigurinë Kibernetike të Rumanisë;
  g. Marrëveshje me Këshillin e Lartë Gjyqësor;

h. Marrëveshje me Air Albania;
i. Marrëveshje me Albpetrol;
j. Marrëveshje me Albsig;
k. Marrëveshje me Agjencinë Kombëtare për Sigurinë Kibernetike të Italisë;
l. Marrëveshje me Institutin Kanadez të Teknologjisë;
m. Marrëveshje me Entin Rregullator të Energjisë;
n. Marrëveshje me Agjencinë Kombëtare të Punësimit dhe Aftësive;
o. Marrëveshje me Fondacionin Shqiptaro Amerikan për Zhvillim - Qendra Protik;
p. Marrëveshje me Qendrën për Mbrojtjen e të Drejtave të Fëmijëve në Shqipëri.

Në nivel ndërkombëtar, Shqipëria ka qenë pjesë aktive e takimeve dhe forumeve me rëndësi strategjike. Në kuadër të Kartës SHBA-Adriatike (A5), gjatë takimit të zhvilluar në Qershor 2024 në Tiranë, u theksua rëndësia e bashkëpunimit të ngushtë me NATO dhe partnerët ndërkombëtarë për ndërtimin e kapaciteteve dhe zhvillimin e politikave të përbashkëta. Më tej, në Shtator 2024, në tryezën "*Policy Roundtable on Integrating the Western Balkans into the European Union Cybersecurity Agency (ENISA)*", u diskutuan hapat për integrimin e rajonit në arkitekturën evropiane të sigurisë kibernetike. Kontributi në *workshop-in* teknik të zhvilluar në bashkëpunim me UNDP (2 - 4 nëntor 2024), si dhe organizimi i "*Western Balkans Cyber Dialogue*" (20 - 21 nëntor 2024), shërbyen si platforma të rëndësishme për shkëmbimin e praktikave të mira dhe për ndërtimin e partneriteteve të qëndrueshme në fushën e sigurisë kibernetike.

Shqipëria ka marrë pjesë në ushtrimin rajonal për bashkëpunim kundër krimit kibernetik ("*Regional Cybercrime Cooperation Exercise*") dhe ka zhvilluar shkëmbime me CERT Poland dhe CERT-et e Ballkanit Perëndimor, duke ndihmuar në ndërtimin e një rrjeti reagues ndaj incidenteve kibernetike. Projekte si "*Strengthening SEE Resilience in Cyber Security"* dhe misionet këshillimore të ISG kanë kontribuar në rritjen e koordinimit ndërinstitucional dhe në ndarjen e ekspertizës mes sektorit publik dhe atij privat. Këto zhvillime e pozicionojnë Shqipërinë si një partner të besueshëm dhe aktiv në arkitekturën e sigurisë kibernetike, si në rajon ashtu edhe në nivel ndërkombëtar, duke ecur drejt objektivit të një mjedisi digjital më të sigurt dhe më të qëndrueshëm.

IV. REKOMANDIME

Për të siguruar një zbatim efektiv të Strategjisë Kombëtare për Sigurinë Kibernetike është e domosdoshme ngritja e një sistemi të qëndrueshëm për monitorimin dhe vlerësimin e saj. Një nga sfidat kryesore aktualisht është mungesa e ndërgjegjësimit të plotë institucional mbi rolin dhe përgjegjësitë që burojnë nga strategjia. Kjo kërkon ndërmarrjen e takimeve informuese për drejtuesit dhe stafin teknik, me qëllim rritjen e njohurive dhe angazhimit të tyre në zbatimin e objektivave të strategjisë.

Një tjetër aspekt thelbësor është krijimi i strukturave të dedikuara për ndjekjen e progresit. Çdo institucion duhet të emërojë një pikë kontakti për sigurinë kibernetike dhe zbatimin e strategjisë, duke siguruar koordinim të brendshëm dhe raportim të rregullt. Kjo do të ndihmojë në identifikimin e sfidave,vonesave dhe praktikave të mira që mund të shkëmbehen.

Në këtë kuadër, një sfidë kritike mbetet mungesa e personelit të specializuar. Pa burime njerëzore të kualifikuara dhe të dedikuara, strategjia nuk mund të zbatohet në mënyrë të qëndrueshme. Nevojitet një analizë e plotë e kapaciteteve ekzistuese dhe më pas ndërhyrje konkrete për rekrutim, trajnime dhe certifikime në fushën e sigurisë kibernetike. Bashkëpunimi me institucionet akademike dhe zhvillimi i programeve të përbashkëta mund të krijojnë një bazë të re profesionistësh të përgatitur për të përballuar sfidat në rritje të sigurisë kibernetike.

Po aq e rëndësishme është rritja e investimeve në teknologji dhe burime njerëzore. Institucionet publike kanë nevojë për teknologji të përditësuar dhe sisteme të integruara të mbrojtjes, të cilat kërkojnë financim të mjaftueshëm dhe të planifikuar në mënyrë strategjike. Përveç infrastrukturës, buxhetet duhet të reflektojnë rëndësinë e trajnimit të vazhdueshëm të stafit dhe ndërtimit të ekipeve të specializuara. Këto investime janë kusht i domosdoshëm për të kaluar nga angazhimet formale drejt rezultateve të matshme.

Së fundi, përfshirja e aktorëve të jashtëm si shoqëria civile dhe sektori privat në procesin e monitorimit do të siguronte transparencë dhe do të sillte përvojë të vlefshme në zbatim. Krijimi i një mekanizmi të hapur për raportim dhe ndarje të progresit mund të forcojë llogaridhënien dhe të stimulojë bashkëpunimin ndërsektorial. Strategjia nuk duhet të jetë vetëm një dokument formal, por një instrument aktiv që drejton transformimin digjital të sigurt dhe të qëndrueshëm të vendit.