REPUBLIKA E SHQIPËRISË

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

RAPORT MONITORIMI PËR VITIN 2025 I STRATEGJISË KOMBËTARE PËR SIGURINË KIBERNETIKE 2025 - 2030 DHE PLANIT TË VEPRIMIT 2025 - 2027

Tiranë, 2026

Përmbajtja

Tabela e Grafikëve

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

SHKURTIME

AKSK	Autoriteti Kombëtar për Sigurinë Kibernetike
SKSK	Strategjia Kombëtare për Sigurinë Kibernetike
MPB	Ministria e Punëve të Brendshme
MEI	Ministria e Ekonomisë dhe Inovacionit
MSHMS	Ministria e Shëndetësisë dhe Mirëqënies
MA	Ministria e Arsimit
MIE	Ministria e Infrastrukturës dhe Energjisë
MEPJ	Ministria për Evropën dhe Punët e Jashtme
MISP	*Malware Information Sharing Platform* Platformë *open-source,* që përdoret për mbledhjen, analizimin dhe shkëmbimin e informacionit mbi kërcënimet kibernetike
MM	Ministria e Mbrojtjes
SHISH	Shërbimi Informativ i Shtetit
DPPSH	Drejtoria e Përgjithshme e Policisë së Shtetit
ASHDMF	Agjencia Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijëve
QKEDH	Qendra e Koordinimit Kundër Ekstremizmit të Dhunshëm
AKEP	Autoriteti Komunikimeve Elektronike dhe Postare
DPA	Drejtoria e Përgjithshme e Akreditimit
AMA	Autoriteti i Mediave Audiovizive
HEDAYAH	*The International Center of Excellence For Countering Extremism and Violent Extremism* Qendra Ndërkombëtare e Ekselencës për Luftën ndaj Ekstremizmit dhe Ekstremizmit të Dhunshëm
PMF	Punonjësi për Mbrojtjen e Fëmijës
SME	Ndërmarrjeve të Vogla dhe të Mesme
CILC	Qendra për Bashkëpunimin Ndërkombëtar Ligjor të Holandës
SEECP	*South-East European Cooperation Process* Procesi i Bashkëpunimit në Evropën Juglindore
NATO	Organizata e Traktatit të Atlantikut të Veriut
DCAF	Qendra e Gjenevës për Qeverisjen e Sektorit të Sigurisë
CERT	Computer Emergency Response Team- Ekipi për Reagim Emergjent ndaj Incidenteve Kompjuterike
eGA	*e-Governance Academy* Akademia e Qeverisjes Elektronike
NUKIB	Agjencia Çeke për Sigurinë e Informacionit
BEREC	*Body of European Regulators for Electronic Communications* Organi i Rregullatorëve Evropianë për Komunikimet Elektronike
ITU	Unioni Ndërkombëtar i Telekomunikacionit

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

PARATHËNIE

Ky raport monitorimi është hartuar mbi bazën e të dhënave zyrtare të raportuara nga strukturat e brendshme të Autoritetit Kombëtar për Sigurinë Kibernetike, si dhe nga institucionet përgjegjëse për monitorimin e zbatimit të masave, në përputhje me Planin e Veprimit 2025-2027.

Dokumenti përbën pjesë të raportimit vjetor mbi ecurinë e zbatimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2025-2030, e miratuar me Vendim të Këshillit të Ministrave nr. 606, datë 23.10.2025, "Për miratimin e Strategjisë Kombëtare për Sigurinë Kibernetike 2025 - 2030 dhe të Planit të Veprimit 2025 - 2027".

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

PËRMBLEDHJE EKZEKUTIVE

Ky raport monitorimi ka për qëllim vlerësimin e progresit të arritur gjatë vitit 2025 në zbatimin e Strategjisë Kombëtare për Sigurinë Kibernetike 2025-2030, përmes analizës së nivelit të realizimit të masave të përcaktuara në Planin e Veprimit 2025-2027.

Gjatë periudhës raportuese, zbatimi i Strategjisë Kombëtare për Sigurinë Kibernetike ka shënuar progres të dukshëm në disa fusha prioritare, veçanërisht në forcimin e kuadrit ligjor dhe rregullator, rritjen e kapaciteteve institucionale dhe teknike si dhe në forcimin e bashkëpunimit ndërinstitucional dhe ndërkombëtar. Një pjesë e konsiderueshme e masave të planifikuara janë realizuar, ndërkohë që masa të tjera vijojnë të jenë në proces të vazhdueshëm zbatimi.

HYRJE

Zhvillimet e shpejta teknologjike, transformimi digjital dhe rritja e ndjeshme e kompleksitetit të kërcënimeve kibernetike kërkojnë një qasje të koordinuar ndërinstitucionale, të integruar dhe të qëndrueshme në nivel kombëtar. Në mbështetje të kësaj qasjeje, të objektivave të qeverisë shqiptare dhe të procesit të transformimit digjital, Autoriteti Kombëtar për Sigurinë Kibernetike ka zbatuar SKSK 2025-2030, miratuar me vendim të Këshillit të Ministrave nr. 606, datë 23.10.2025, "Për Miratimin e Strategjisë Kombëtare Për Sigurinë Kibernetike 2025-2030 dhe të Planit të Veprimit 2025-2027", e cila synon realizimin e pesë politikave, si vijon:

- Politika 1: Mbrojtja e Infrastrukturës Digjitale;
- Politika 2: Mbrojtja *Online* e Qytetarëve dhe Nxitja e Kulturës Kibernetike;
- Politika 3: Forcimi i Bashkëpunimit Ndërkombëtar;
- Politika 4: Nxitja e Inovacionit dhe Kërkimit Shkencor në Sigurinë Kibernetike;
- Politika 5: Mbrojtja ndaj Kërcënimeve Hibride.

Aktorët e zbatimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2025-2030 janë:

- Autoriteti Kombëtar për Sigurinë Kibernetike;
- Ministria e Punëve të Brendshme;
- Ministria e Ekonomisë dhe Inovacionit;
- Ministria e Shëndetësisë dhe Mirëqënies Sociale;
- Ministria e Arsimit;
- Ministria e Infrastrukturës dhe Energjisë;
- Ministria për Evropën dhe Punët e Jashtme;
- Ministria e Mbrojtjes;
- Agjencia Kombëtare e Shoqërisë së Informacionit;
- Shërbimi Informativ i Shtetit;
- Drejtoria e Përgjithshme e Policisë së Shtetit;
- Agjencia Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijëve;
- Qendra e Koordinimit Kundër Ekstremizmit të Dhunshëm;
- Autoriteti Komunikimeve Elektronike dhe Postare;
- Drejtoria e Përgjithshme e Akreditimit;
- Autoriteti i Mediave Audiovizive.

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

SKSK 2025-2030 ka parashikuar për zbatim gjatë pesë viteve të implementimit të saj, 5 Politika, 29 Objektiva Specifik, 113 Masa dhe ky raport paraqet një analizë të thellë mbi progresin dhe realizimin e tyre gjatë vitit 2025.

Zbatimi i SKSK 2025-2030 është arritur përmes një sistemi monitorimi dhe vlerësimi për të verifikuar progresin në plotësimin ose jo të objektivave specifikë dhe masave të vendosura në Planin e Veprimit. Me qëllim zbatimin dhe vlerësimin periodik të SKSK 2025-2030, AKSK harton raportin vjetor të monitorimit sipas kontributit nga secili institucion përgjegjës.

Në këtë kuadër, raporti synon të ofrojë një pasqyrë të qartë, të matshme dhe të krahasueshme të progresit kombëtar, duke shërbyer si instrument mbështetës për vendimmarrjen strategjike, për forcimin e transparencës, llogaridhënies dhe bashkëpunimit ndërinstitucional.

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. Këto rezultate lidhen drejtpërdrejt me zbatimin e pesë politikave të Strategjisë, ku secili institucion ka raportuar mbi nivelin e realizimit të objektivave dhe masave përkatëse, mbi sfidat e hasura dhe vlerësimin e përgjithshëm të progresit në zbatimin e strategjisë.

PROCESI I MONITORIMIT

Procesi i ndjekur për hartimin e Raportit të Monitorimit përshkruan hapat dhe mënyrën e realizimit të tij, me synim ofrimin e udhëzimeve të qarta që lehtësojnë kuptueshmërinë e përmbajtjes dhe orientojnë paraqitjen e rezultateve kryesore. Autoriteti Kombëtar për Sigurinë Kibernetike ka bashkëpunuar në mënyrë të vazhdueshme me institucionet e përfshira në këtë Strategji, duke zbatuar Planin e Veprimit 2025-2027 të përshtatur sipas natyrës dhe specifikave të çdo strukture, me qëllim garantimin e informacionit të saktë dhe gjithëpërfshirës lidhur me:

a. Nivelin e zbatimit të çdo mase (aktivitetet e realizuara për vitin 2025, në proces, si dhe një përshkrim të aktiviteteve të realizuara ose një argumentim për mosrealizimin ose realizimin e pjesshëm të tyre);
b. Informacion mbi realizimin e deritanishëm për aktivitetet në proces (masa në % e realizimit) dhe parashikimin për përmbylljen e tyre;
c. Parashikimi për aktivitetet të cilat rezultojnë të parealizuara ende.

Zbatueshmëria e masave dhe aktiviteteve të Planit të Veprimit 2025-2027 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	Si të parealizuara 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.

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

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 në progresin apo zbatimin e masave të parashikuara në dokumentet strategjike. Ky klasifikim mundëson gjithashtu një analizë të qartë të performancës dhe identifikimin e masave që kërkojnë ndërhyrje të mëtejshme.

Vlerësimi i performancës është bazuar në tregues sasiorë dhe cilësorë, të cilët matin progresin në nivel masash, objektivash specifikë dhe politikash të Strategjisë. Indikatorët e përdorur përfshijnë, ndër të tjera, përqindjen e realizimit të masave, nivelin e përmbushjes së objektivave strategjikë, shkallën e funksionalitetit të kapaciteteve teknike dhe institucionale, si dhe ndikimin e masave në përmirësimin e sigurisë kibernetike në nivel kombëtar.

Për të lehtësuar interpretimin e rezultateve, është përdorur një qasje vizuale përmes grafikëve dhe tabelave përmbledhëse, duke reflektuar progresin sipas politikave dhe sektorëve përkatës.

MASA TË IMPLEMENTUARA NË VITIN 2025

Viti 2025 ka shënuar arritje të rëndësishme dhe progres në fushat kryesore të Strategjisë Kombëtare për Sigurinë Kibernetike (SKSK), të cilat janë reflektuar në rezultate konkrete dhe kanë ndikuar drejtpërdrejt në avancimin e zbatimit të politikave strategjike të saj. Krahas këtyre zhvillimeve pozitive, janë identifikuar edhe sfida të caktuara që kanë ndikuar në nivelin e performancës së disa objektivave specifikë. Masat dhe aktivitetet e paraqitura në vijim pasqyrojnë hapat dhe projektet e realizuara në kuadër të zbatimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2025-2030 për periudhën raportuese, të strukturuara sipas politikave përkatëse.

QËLLIMI I POLITIKËS 1

MBROJTJA E INFRASTRUKTURËS DIGJITALE (PROCESET, KAPACITETET NJERËZORE DHE TEKNOLOGJIA)

Qëllimi i kësaj politike është të sigurojë mbrojtjen, qëndrueshmërinë dhe funksionimin e pandërprerë të infrastrukturës digjitale kombëtare, përmes forcimit të proceseve institucionale, zhvillimit të kapaciteteve njerëzore dhe përdorimit të teknologjive të avancuara të sigurisë kibernetike, me synim parandalimin, zbulimin dhe menaxhimin efektiv të kërcënimeve dhe incidenteve kibernetike.

Objektivat e Politikës 1 fokusohen në:

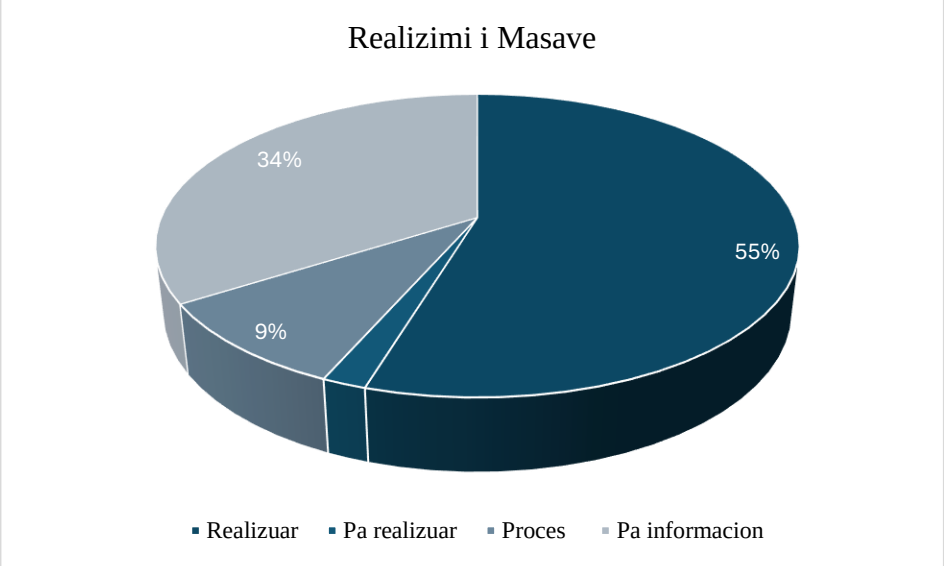
- forcimin e qeverisjes kibernetike dhe përmirësimin e proceseve të menaxhimit të rreziqeve dhe incidenteve kibernetike;
- rritjen e kapaciteteve monitoruese, parandaluese dhe reaguese për mbrojtjen e sistemeve dhe infrastrukturave digjitale;
- garantimin e sigurisë dhe besueshmërisë së transaksioneve elektronike përmes shërbimeve të besuara dhe skemave të certifikimit të sigurisë kibernetike;

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

- zhvillimin e kapaciteteve njerëzore përmes promovimit të kulturës kibernetike dhe rritjes së aftësive profesionale;
- integrimin e teknologjive të avancuara për monitorim, zbulim dhe mbrojtje kibernetike;
- zbatimin e parimit *secure by design* në projektimin dhe zhvillimin e infrastrukturave digjitale;
- menaxhimin e rreziqeve që lidhen me teknologjitë e vjetruara dhe përdorimin e masave kompensuese për garantimin e sigurisë kibernetike.

Gjatë vitit 2025, Plani i Veprimit 2025-2027 për Politikën 1, parashikon zbatimin e gjithsej 53 masave. Nga të cilat, siç vërehet edhe nga Grafiku 1:

- 55% e Masave janë realizuar plotësisht;
- 9% e Masave janë në process;
- 2% e Masave të pa realizuara;
- 34% e Masave nuk disponohet informacion[1].



Grafiku 1. Realizimi i Masave të Politikës 1

Përsa i përket përmbushjes së Objektivave Specifikë të kësaj Politike:

- **Objektivi Specifik 0.1**: Hartimi dhe zbatimi i kuadrit ligjor për Sigurinë , përqendrohet në forcimin e kuadrit ligjor dhe institucional për sigurinë kibernetike përmes hartimit të akteve nënligjore në zbatim të ligjit përkatës, harmonizimit të legjislacionit kombëtar me *acquis* të BE-së, zhvillimit të marrëveshjeve kombëtare dhe ndërkombëtare në këtë fushë, si dhe mbikëqyrjes së zbatimit të ligjit përmes kontrolleve periodike ndaj Infrastrukturave Kritike dhe të Rëndësishme të Informacionit, (OIKI/OIRI);
- **Objektivi Specifik 1.1**: Synon forcimin e kapaciteteve monitoruese dhe mbrojtëse të sistemeve, përmirësimin e qeverisjes kibernetike dhe menaxhimit të

[1] Kjo përqindje vjen si rezultat i mungesës së informacionit,pasi masat e NënObjektivit Specifik. 1.1.6 Implementimi i Skemës së Certifikimit të Sigurisë Kibernetike, janë parashikuar për vitet e ardhshme

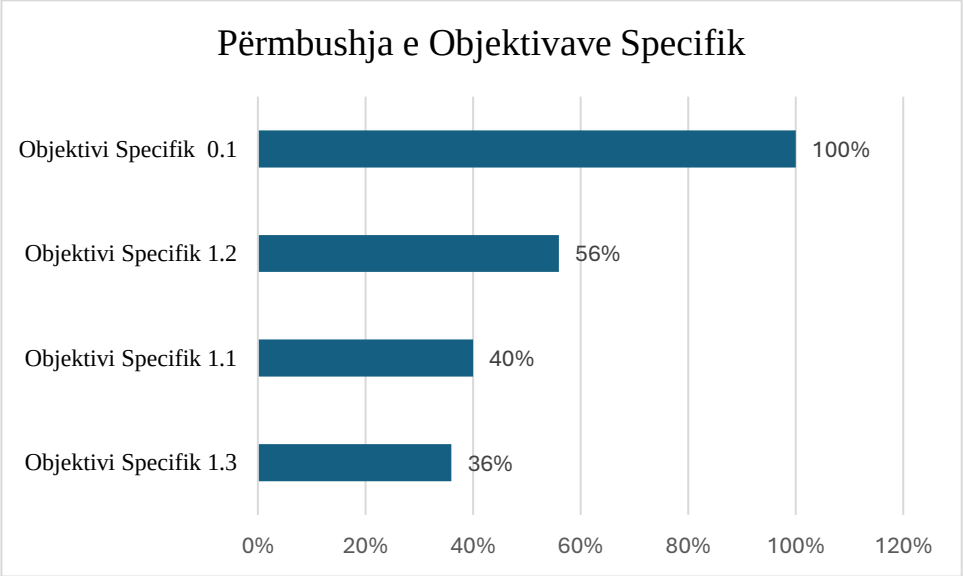
Adresa: Rruga "Papa Gjon Pali II", Nr. 3, Kati 1, Tiranë
Faqe web: www.aksk.gov.al | E-mail: info@aksk.gov.al
Tel./Fax: 04 2221 039

rreziqeve, zhvillimin e planeve për reagimin ndaj incidenteve, garantimin e transaksioneve elektronike përmes shërbimeve të besuara dhe zbatimin e skemës së certifikimit të sigurisë kibernetike;

- **Objektivi Specifik 1.2**: Synon forcimin e kapaciteteve njerëzore përmes promovimit dhe zhvillimit të kulturës kibernetike, si dhe rritjes së aftësive dhe kompetencave profesionale në fushën e sigurisë kibernetike;
- **Objektivi Specifik 1.3**: Synon forcimin e dimensionit teknologjik të sigurisë kibernetike përmes përdorimit dhe integrimit të teknologjive të avancuara, rritjes së kapaciteteve për monitorim, zbulim dhe mbrojtje kibernetike, zbatimit të parimit *secure by design* në infrastrukturat digjitale, menaxhimit efektiv të teknologjive të vjetruara dhe përdorimit të teknologjive alternative kompensuese për reduktimin e rreziqeve kibernetike.

Nga analiza rezulton se:

- Objektivi Specifik 0.1 është realizuar në masën 100%;
- Objektivi Specifik 1.1 është realizuar në masën 56%;
- Objektivi Specifik 1.2 është realizuar në masën 60%;
- Objektivi Specifik 1.3 është realizuar në masën 36%;



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 2025-2027, në lidhje me Politikën 1 janë:

- Hartimi i të gjitha akteve nënligjore në zbatim të Ligjit nr. 25/2024 *"Për sigurinë kibernetike"*, me 20 akte të miratuara;
- Hartimi i projektligjit "*Për identifikimin elektronik, shërbimet e besuara dhe Portofolin e Identitetit Digjital*", në kuadër të harmonizimit të kuadrit ligjor me *acquis* të Bashkimit Evropian, aktualisht në procedurë miratimi në Këshillin e Ministrave;

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

- Konsolidimi i kuadrit rregullator përmes miratimit të vendimit të Këshillit të Ministrave nr. 531, datë 25.09.2025 "Për përmbajtjen dhe mënyrën e dokumentimit të masave organizative, teknike dhe operacionale të sigurisë kibernetike dhe kategorizimin e afateve të masave korrigjuese në infrastrukturat kritike dhe të rëndësishme të informacionit";
- Standardizimi i vlerësimit të rrezikut kibernetik në nivel kombëtar përmes vendimit të Këshillit të Ministrave nr. 308/2025 dhe realizimi i vlerësimeve periodike të rrezikut;
- Miratimi i vendimit të Këshillit të Ministrave nr.813, datë 30.12.2025 "Për miratimin e Skemës Kombëtare të Certifikimit të Sigurisë Kibernetike, si dhe të niveleve të sigurisë së skemës";
- Realizimi i 65 kontrolleve *onsite* dhe *online* ndaj OIKI/OIRI për verifikimin e zbatimit të masave të sigurisë kibernetike nga Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK);
- Përmirësimi i reagimit ndaj incidenteve kibernetike përmes proceseve të Qendrës së Operacionale të Sigurisë (SOC) dhe mekanizmave të eskalimit institucional;
- Krijimi i Sektorit të Analizës, Monitorimit dhe Operimit 24/7 pranë Drejtorisë së Hetimit të Krimit Kibernetik, për monitorimin e kërcënimeve kibernetike në hapësirën digjitale të Shqipërisë përmes inteligjencës kibernetike, duke përfshirë rrjetin e hapur, rrjetet e mbyllura dhe *dark web*;
- Hartimi i Raportit Kombëtar të Rrezikut të Sigurisë Kibernetike, me fokus proceset, teknologjinë dhe faktorët njerëzorë;
- Nënshkrimi i 3 Marrëveshjeve në nivel kombëtar në fushën e sigurisë kibernetike, pas miratimit të Strategjisë Kombëtare të Sigurisë Kibernetike, si dhe vijimi i procesit të bashkëpunimit;
- Bashkëpunim ndërinstitucional ndërmjet Ministrisë së Arsimit, Ministrisë së Punëve të Brendshme, institucioneve të varësisë dhe partnerëve ndërkombëtarë në fushën e parandalimit e radikalizmit të ekstremizmit të dhunshëm *online*;
- Zhvillimi i 40 trajnimeve dhe aktiviteteve me 7,097 pjesëmarrës për ngritjen e kapaciteteve profesionale në fushën e sigurisë kibernetike;
- Realizimi i trajnimeve praktike dhe simulimeve teknike (laboratorë, CTF, SimSpace) për forcimin e aftësive profesionale;
- Zhvillimi i fushatave dhe trajnimeve për higjienën kibernetike dhe praktikat e mira të sigurisë për punonjësit dhe qytetarët;
- Ndërmarrja e masave për integrimin e sigurisë kibernetike në arsimin parauniversitar, përmes aktiviteteve edukative dhe përditësimit të kurrikulave;
- Ndërhyrje të koordinuara dhe të qëndrueshme në institucionet arsimore parauniversitare për ngritjen e kapaciteteve të stafeve shkollore dhe parandalimin e radikalizimit dhe ekstremizmit të dhunshëm online;
- Zhvillimi i fushatave sensibilizuese dhe ndërgjegjësuese për nxënësit dhe prindërit mbi rreziqet e ekstremizmit të dhunshëm online, gjuhën e urrejtjes dhe manipulimin në rrjetet sociale;
- Zbatim i aktiviteteve informuese përmes orëve tematike dhe angazhimit të shërbimit psiko-social, oficerëve të sigurisë dhe Policisë të Shtetit;
- Konsolidimi i rolit të shkollës si hapësirë e sigurt për zhvillimin e mendimit kritik, tolerancës dhe rezistencës ndaj ideologjive të dhunshme në mjedisin digjital;

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

- Nisja e procesit të rishikimit dhe përditësimit të kurrikulave të arsimit parauniversitar, në zbatim të urdhrit nr. 610, datë 20.12.2024 të Ministrisë së Arsimit dhe Sportit, me fokus integrimin e sigurisë kibernetike dhe qytetarisë digjitale;
- Integrimi i strukturuar i sigurisë kibernetike në programet e reja të miratuara të lëndës së Teknologjisë së Informacionit dhe Komunikimit (TIK) për arsimin fillor;
- Miratimi i programeve lëndore të TIK-ut për klasat I–V, ku siguria kibernetike përfshihet si pjesë përbërëse e kurrikulës;
- Përfshirja e tematikave mbi sigurinë gjatë përdorimit të kompjuterit dhe internetit të sigurt në programet mësimore për nxënësit e ciklit fillor.

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

- Përfshirja e pritshme e tematikave të sigurisë kibernetike në programet e reja të lëndës së Teknologjisë së Informacionit dhe Komunikimit (TIK) për arsimin e mesëm të ulët dhe arsimin e mesëm të lartë, aktualisht në fazë hartimi, me synim sigurimin e një trajtimi të vazhdueshëm dhe progresiv të këtyre çështjeve në të gjitha nivelet e arsimit parauniversitar.

INFORMACION MBI ZBATIMIN E MASAVE

Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK)

Gjatë vitit 2025, ka zbatuar në mënyrë efektive dhe të koordinuar Politikën 1, Mbrojtja e Infrastrukturës Digjitale (Proceset, Kapacitetet Njerëzore dhe Teknologjia), përmes forcimit të kapaciteteve parandaluese, reaguese, mbikëqyrëse dhe rregullatore në nivel kombëtar. Në aspektin operativ, është evidentuar një rritje e ndjeshme e aftësisë për reagim në kohë reale ndaj incidenteve kibernetike, si rezultat i përmirësimit të proceseve të Qendrës Operacionale të Sigurisë (SOC), duke mundësuar koordinim institucional më të strukturuar dhe trajtim parandalues të kërcënimeve kibernetike. Paralelisht, AKSK ka forcuar funksionin analitik dhe inteligjent përmes përdorimit të platformave të avancuara të *Cyber Threat Intelligence* (CTI) me bazë teknologjitë e inteligjencës artificiale duke siguruar mbledhje, korrelacion dhe analizë të automatizuar të të dhënave.

Në këtë kuadër, është rritur ndjeshëm ndërgjegjësimi mbi situatën aktuale të sigurisë kibernetike përmes përdorimit të platformës *MISP NATO*, në bashkëpunim me Ministrinë e Mbrojtjes, si dhe përmes hartimit të raporteve për investigimin e thellë të sulmeve kibernetike, veçanërisht në sistemet e ruajtjes së të dhënave. Po ashtu, gjatë vitit 2025 është përfunduar krijimi dhe përditësimi i laboratorit të sigurisë kibernetike pranë AKSK, duke rritur kapacitetet për testim, simulim dhe analizë të skenarëve të kërcënimeve kibernetike. Dimensioni mbikëqyrës është intensifikuar ndjeshëm, ku janë realizuar 65 kontrolle *onsite* dhe *online* ndaj operatorëve të Infrastrukturave Kritike dhe të Rëndësishme të Informacionit (OIKI/OIRI), për verifikimin e zbatimit të masave organizative, teknike dhe operacionale të sigurisë kibernetike, si dhe identifikimin e boshllëqeve në teknologji, procese dhe burime njerëzore. Në vijim të masave korrigjuese, pas identifikimit të hendekëve teknologjikë, janë zhvilluar takime dhe orientime teknike me 16 institucione të administratës publike, për promovimin e përdorimit të platformave

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

alternative dhe reduktimin e varësisë nga teknologjitë e vjetruara, përfshirë aspektet e *end-of-life* (EOL) të teknologjive. Në kuadër të këtij procesi, takimet dhe orientimet teknike janë realizuar me institucionet e mëposhtme:

1. Institucioni i Prefektit të Qarkut Durrës (IDP);
2. Këshilli i Lartë Gjyqësor (KLGJ);
3. Kontrolli i Lartë i Shtetit (KLSH);
4. Presidenca e Republikës;
5. Këshilli i Lartë i Prokurorisë (KLP);
6. Instituti i Statistikave (INSTAT);
7. Kuvendi i Republikës së Shqipërisë;
8. Gjykata Kushtetuese;
9. Agjencia Shtetërore e Diasporës (ASD);
10. Bashkia Shkodër;
11. Zyra Vendore e Operatorit të Shërbimit Kombëtar të Punësimit – Skrapar (OSHKSH Skrapar);
12. Shkolla e Magjistraturës;
13. Komisioni Qendror i Zgjedhjeve (KQZ);
14. Inspektorati i Lartë i Deklarimit dhe Kontrollit të Pasurive dhe Konfliktit të Interesit (ILDKPKI);
15. Njësia e Inteligjencës Financiare (FIU);
16. Prokuroria e Përgjithshme.

Në aspektin ligjor dhe rregullator, është shënuar progres i konsiderueshëm në forcimin e kuadrit normativ të sigurisë kibernetike. Në zbatim të Objektivit Specifik 0.1 – Hartimi dhe zbatimi i kuadrit ligjor për Sigurinë Kibernetike, është realizuar plotësisht hartimi i akteve nënligjore në zbatim të Ligjit nr. 25/2024 *"Për Sigurinë Kibernetike",* ku 20 akte nënligjore janë miratuar. Paralelisht, pas miratimit të **Strategjisë Kombëtare për Sigurinë Kibernetike**, është avancuar bashkëpunimi institucional përmes nënshkrimit të 3 Marrëveshjeve në nivel kombëtar, ndërkohë që procesi i zgjerimit të bashkëpunimit vijon. Gjithashtu, harmonizimi i kuadrit ligjor me *acquis* të Bashkimit Evropian ka shënuar progres të pjesshëm, përmes hartimit të projektligjit *"Për identifikimin elektronik, shërbimet e besuara dhe Portofolin e Identitetit Digjital*", aktualisht në Këshillin e Ministrave për ndjekjen e procedurave të miratimit. Në vijim të forcimit të mekanizmave rregullatorë dhe mbikëqyrës, në kuadër të **Nënobjektivit Specifik 1.1.6** – Implementimi i Skemës së Certifikimit të Sigurisë Kibernetike, është realizuar plotësisht me miratimin e vendimit të Këshillit të Ministrave nr.813, datë 30.12.2025 "Për miratimin e skemës kombëtare të certifikimit të sigurisë kibernetike, si dhe të niveleve të sigurisë së skemës", duke krijuar një bazë të qëndrueshme për standardizimin dhe certifikimin e sigurisë kibernetike në nivel kombëtar.

Në drejtim të rritjes së kapaciteteve njerëzore, AKSK ka zbatuar një program të gjerë trajnimesh dhe ndërgjegjësimi. Gjatë periudhës janar-shtator 2025, janë zhvilluar pesë trajnime mbi Higjienën Kibernetike dhe Praktikat më të Mira të Sigurisë, në bashkëpunim me CRDF Global dhe me mbështetjen e Departamentit Amerikan të Shtetit, të organizuara në Gjirokastër, Berat, Durrës, Elbasan dhe Tiranë, me pjesëmarrjen e mbi 2,100 individëve nga institucionet

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

publike si në formë fizike ashtu edhe *online*. Paralelisht, gjatë periudhës mars-shtator 2025, janë zhvilluar një seri *workshop*-esh dhe trajnimesh profesionale tematike, përfshirë *workshop*-in për sigurinë kibernetike në rrjetin 5G, analizën e kërcënimeve sipas raportit ENISA 2030, politikat e edukimit digjital dhe praktikat më të mira ndërkombëtare të sigurisë kibernetike. Nga muaji tetor-dhjetor 2025 janë realizuar 4 takime me Infrastrukturat Kritike dhe të Rëndësishme të Informacionit, me tematika: "Qeverisja e mirë kibernetike dhe implementimin e masave të sigurisë kibernetike", "Legjislacioni në fushën e sigurisë kibernetike", "Menaxhimi i Rrezikut Kibernetik dhe Vlerësimi i Tij", "Monitorimin dhe Simulimin Proaktiv", "Menaxhimi i Incidenteve & Menaxhimi Krizave Kibernetike". Po ashtu, gjatë vitit 2025 janë zhvilluar 8 webinare, të cilat kanë përfshirë në total 4,781 pjesëmarrës.

Në funksion të zhvillimit të talenteve të reja, janë organizuar aktivitete të dedikuara për të rinjtë, përfshirë përgatitjen dhe pjesëmarrjen e ekipit shqiptar në "*European Cyber Security Challenge"(ECSC)*, si dhe zhvillimin e *Western Balkans Cyber Camp* në Durrës, me pjesëmarrës nga vendet e rajonit.

Në total, gjatë vitit 2025 janë realizuar 40 trajnime dhe aktivitete me gjithsej 7,097 pjesëmarrës, përfshirë ushtrime praktike (*CTF*), aktivitete laboratorike, *webinare* dhe ushtrime simulimi, me fokus menaxhimin e incidenteve dhe krizave kibernetike, qeverisjen dhe menaxhimin e rrezikut kibernetik, ushtrime të tipit *tabletop* (TTX) dhe skenarë praktikë reagimi. Në vijimësi, janë zhvilluar takime të dedikuara me 16 infrastruktura kritike dhe të rëndësishme, mbi bazën e të cilave është hartuar një plan trajnimesh specifike për rritjen e qëndrueshmërisë kibernetike dhe zbatimin e metodave alternative të mbrojtjes.

Së fundi, në funksion të harmonizimit ligjor dhe përafrimit me zhvillimet e reja teknologjike, AKSK ka dhënë kontribut aktiv në hartimin e projektligjit *"Për tregjet e Kripto Aseteve"*, duke adresuar risitë dhe nevojën për përshtatje të kuadrit rregullator në rast ndërveprimi me fushën e sigurisë kibernetike, në përputhje me prioritetet strategjike kombëtare dhe standardet evropiane.

Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI)

Në kuadër të forcimit të sigurisë kibernetike, rritjes së besueshmërisë së shërbimeve digjitale dhe përafrimit me standardet ndërkombëtare, AKSHI ka ndërmarrë një sërë veprimesh të rëndësishme dhe të qëndrueshme me ndikim të drejtpërdrejtë në infrastrukturën qeveritare dhe shërbimet publike digjitale.

AKSHI ka siguruar vazhdimësinë e certifikimit, riauditimit dhe ricertifikimit sipas standardeve ndërkombëtare ISO, duke përfshirë ISO 37001 për menaxhimin kundër korrupsionit, ISO 27001 për sigurinë e informacionit, ISO 9001 për menaxhimin e cilësisë dhe ISO 20000-1 për menaxhimin e shërbimeve IT. Paralelisht, është realizuar auditimi për konformitet ndaj rregullores eIDAS për shërbimet e besuara, duke garantuar përputhshmërinë e shërbimeve digjitale me kërkesat evropiane. Këto procese janë zhvilluar përmes kontratave përkatëse të viteve 2022 dhe 2024, duke reflektuar një qasje të vazhdueshme për përmirësim dhe konsolidim institucional.

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

Në funksion të mbrojtjes së infrastrukturës kritike shtetërore, AKSHI ka rinovuar shërbimin e mbrojtjes kibernetike për rrjetin qeveritar, përmes një kontrate të klasifikuar, duke garantuar mbrojtjen e vazhdueshme ndaj kërcënimeve kibernetike dhe rritjen e gatishmërisë operacionale të sistemeve shtetërore. Njëkohësisht, është siguruar rinovimi i mirëmbajtjes së sistemeve të sigurisë të implementuara pranë AKSHI-t, me qëllim ruajtjen e funksionalitetit, qëndrueshmërisë dhe efikasitetit të masave teknike të sigurisë.

Në nivel strategjik, AKSHI ka kontribuar gjithashtu në zbatimin e partneriteteve ndërkombëtare me rëndësi të veçantë për transformimin digjital dhe sigurinë e ekosistemit qeveritar IT. Në këtë kuadër, janë zbatuar vendimet e Këshillit të Ministrave për miratimin dhe ndryshimin e marrëveshjes së rinovuar të partneritetit strategjik ndërmjet Këshillit të Ministrave të Republikës së Shqipërisë dhe *Microsoft Corporation*, duke mbështetur modernizimin e platformave digjitale, rritjen e sigurisë së informacionit dhe adoptimin e praktikave më të mira ndërkombëtare.

Në tërësi, këto masa dëshmojnë rolin aktiv dhe kontributin thelbësor të AKSHI-t në ndërtimin e një infrastrukture digjitale të sigurt, të standardizuar dhe të qëndrueshme, në funksion të shërbimeve publike moderne dhe forcimit të sigurisë kibernetike në nivel kombëtar.

Ministria e Arsimit (MA)

Në bashkëpunim të ngushtë me institucionet e varësisë, Ministrinë e Punëve të Brendshme, institucionet e saj të varësisë, AKSK dhe partnerë të tjerë institucionalë e ndërkombëtarë, ka dhënë një kontribut të rëndësishëm në zbatimin e Politikës 1: Kapacitetet Njerëzore, në veçanti në kuadër të Nënobjektivit Specifik 1.2.2 – Rritja e kapaciteteve profesionale. Në këtë kuadër, janë ndërmarrë hapa të qëndrueshme dhe të koordinuar në institucionet arsimore parauniversitare, me synim ngritjen e kapaciteteve të stafeve shkollore dhe sensibilizimin e nxënësve kundër radikalizimit dhe ekstremizmit të dhunshëm *online*, në përputhje me prioritetet kombëtare të sigurisë, arsimit dhe mbrojtjes së fëmijëve.
Në kuadër të zbatimit të Politikës 1: Kapacitetet Njerëzore, janë ndërmarrë masa të qëndrueshme dhe të koordinuara në institucionet arsimore parauniversitare për parandalimin dhe adresimin e formave të dhunës *online*, përfshirë radikalizimin dhe ekstremizmin e dhunshëm *online*, gjuhën e urrejtjes, manipulimin përmes rrjeteve sociale dhe ekspozimin ndaj përmbajtjeve të dëmshme. Aktivitetet sensibilizuese dhe ndërgjegjësuese të zhvilluara gjatë vitit 2025 në të gjitha Drejtoritë Rajonale të Arsimit Parauniversitar (DRAP) kanë synuar rritjen e ndërgjegjësimit të nxënësve, mësuesve dhe prindërve mbi rreziqet dhe pasojat psikologjike, sociale dhe arsimore të dhunës në mjedisin digjital.

Këto ndërhyrje janë realizuar përmes orëve tematike dhe edukative, diskutimeve të hapura, aktiviteteve praktike dhe përfshirjes së shërbimit psiko-social, duke forcuar aftësitë për identifikimin, parandalimin dhe raportimin e rasteve të dhunës online dhe duke konsoliduar rolin e shkollës si një hapësirë e sigurt për mbrojtjen e fëmijëve në mjedisin digjital.

Në kuadër të zbatimit të projektit "Përmirësimi i aksesit të barabartë në shërbimet publike me standard të lartë nëpërmjet operacionit GOVTECH", janë trajnuar 830 mësues të arsimit fillor lidhur me elementët e përgjithshëm të sigurisë në web dhe etikës digjitale. Këto trajnime janë zhvilluar si pjesë e paketës së moduleve për aftësitë digjitale të nivelit bazë,

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

bazuar në Standardet Profesionale të Përdorimit të TIK-ut. Gjithashtu, në mbështetje të trajnimit të vazhduar, mësuesit e arsimit fillor janë trajnuar me një modul specifik për Etikën Digjitale dhe Sigurinë në Teknologji, me një ngarkesë prej 12 orësh trajnim të drejtpërdrejtë.

Referuar ngritjes së kapaciteteve të drejtuesve të rrjeteve profesionale, janë trajnuar rreth 26 drejtues të rrjeteve profesionale, me fokus të veçantë në çështjet e sigurisë në internet, mbrojtjen në mjedisin digjital dhe rolin e tyre në përhapjen e praktikave të sigurta në komunitetet profesionale të mësuesve.

Kurrikula e re e TIK-ut përmban një tematikë të posaçme të titulluar "Siguria e të punuarit në kompjuter", e cila synon zhvillimin e aftësive të nxënësve për përdorimin e sigurt dhe etik të teknologjisë. Referuar zhvillimit profesional të mësuesve të TIK-ut për zbatimin e kurrikulës së re për vitin shkollor 2025- 2026, pritet që të trajnohen rreth 914 mësues.

Sipas të dhënave të raportuara nga drejtoritë rajonale të arsimit parauniversitar janë mbi 48 000 prindër që kanë marrë pjesë në aktivitetet/veprimtaritë e realizuara nga shkollat për radikalizimin, ekstremizmin online, përdorimin e sigurt të internetit dhe platformave të sigurisë kibernetike.

Ministria e Mbrojtjes (MM)

Në kuadër të zbatimit të nën-objektivave të Strategjisë Kombëtare për Sigurinë Kibernetike, gjatë vitit 2025 Ministria e Mbrojtjes, në bashkëpunim të ngushtë me AKSK dhe institucionet e tjera përgjegjëse, ka ndërmarrë një sërë masash me fokus forcimin e monitorimit, reagimit dhe mbrojtjes ndaj kërcënimeve kibernetike dhe hibride.

Në kuadër të NënObjektivit 1.1.2.2, monitorimi i kërcënimeve kibernetike në hapësirën digjitale të Republikës së Shqipërisë është realizuar përmes shkëmbimit të vazhdueshëm të informacionit dhe inteligjencës kibernetike, duke shfrytëzuar kapacitetet ekzistuese në fushën e inteligjencës dhe mekanizmat e koordinimit ndërinstitucional.

Sa i përket NënObjektivit 1.1.4.5, gjatë vitit 2025 janë ndërmarrë hapa të rëndësishëm strukturorë për përmirësimin e gjurmimit dhe analizimit të sulmeve kibernetike. Këto masa përfshijnë krijimin e strukturave të dedikuara për reagimin dhe menaxhimin e incidenteve, përfshirë Komandën Kibernetike dhe Ndërlidhjen, si dhe pajisjen e strukturave të Ministrisë së Mbrojtjes dhe Forcave të Armatosura me mjete të lëvizshme për reagim ndaj incidenteve dhe analiza forenzike.

Në kuadër të NënObjektivit 1.3.2.1, ndonëse gjatë vitit 2025 nuk janë realizuar investime të reja financiare, janë shfrytëzuar kapacitetet ekzistuese teknike për rritjen e mbrojtjes proaktive ndaj kërcënimeve të avancuara të vazhdueshme (APT). Konkretisht, në sistemet aktuale të monitorimit të sigurisë (SIEM/SOAR) janë integruar platforma të inteligjencës së kërcënimeve ("threat intelligence feeds"), duke përmirësuar aftësinë për zbulim të hershëm dhe analizë të kërcënimeve.

Drejtoria e Përgjithshme e Policisë së Shtetit (DPPSH)

Në kuadër të forcimit të kapaciteteve kombëtare për sigurinë kibernetike, DPPSH ka dhënë një kontribut të rëndësishëm në monitorimin e kërcënimeve kibernetike në hapësirën digjitale të

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

Republikës së Shqipërisë. Për këtë qëllim, është krijuar Sektori i Analizës, Monitorimit dhe Shërbimit 24/7, pranë Drejtorisë së Hetimit të Krimit Kibernetik, me mision monitorimin, analizimin dhe identifikimin në kohë reale të kërcënimeve kibernetike përmes përdorimit të inteligjencës kibernetike.

Ky sektor realizon monitorimin sistematik të kërcënimeve kibernetike në rrjetin e hapur (*open web*), rrjetet e mbyllura dhe *dark web*, duke mundësuar grumbullimin, analizimin dhe vlerësimin e informacionit për rreziqet dhe aktivitetet keqdashëse në mjedisin digjital. Nëpërmjet këtyre kapaciteteve, Policia e Shtetit kontribuon në forcimin e parandalimit, zbulimit të hershëm dhe reagimit ndaj incidenteve dhe veprimtarive kriminale kibernetike, si dhe në mbështetjen e bashkëpunimit ndërinstitucional për rritjen e sigurisë kibernetike në nivel kombëtar.

Drejtoria e Përgjithshme e Akreditimit (DPA)
Në zbatim të Objektivit specifik 0.1 "Hartimi dhe zbatimi i kuadrit ligjor për Sigurinë Kibernetike", Drejtoria e Përgjithshme e Akreditimit (DPA), ka kontribuar në mënyrë aktive në procesin e hartimit të draft-legjislacionit dhe kuadrit rregullator në fushën e sigurisë kibernetike në nivel kombëtar, përmes dhënies së mendimeve dhe komenteve mbi dokumentet e propozuara nga Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK) dhe Kryeministria.

Lidhur me nënobjektivin 1.1.6.2 "Akreditimi i Organeve të Vlerësimit të Konformitetit (OVK)", për të cilin institucioni përgjegjës është përcaktuar DPA, theksohet se ky objektiv është parashikuar në kuadër të kërkesave dhe pritshmërive për zhvillimin e mëtejshëm të sistemit të akreditimit dhe forcimin e infrastrukturës kombëtare të cilësisë në fushën e sigurisë kibernetike. DPA e vlerëson këtë objektiv si të rëndësishëm për zhvillimet afatmesme dhe afatgjata në këtë fushë. Aktualisht, DPA ndodhet në fazën përgatitore për hapjen e aktivitetit të akreditimit të trupave të certifikimit të produktit dhe ende nuk ka filluar zbatimin e kësaj skeme akreditimi gjatë vitit 2025.

Autoriteti Komunikimeve Elektronike dhe Postare (AKEP)
Në kuadër të zbatimit të kësaj mase, AKEP ka dhënë një kontribut të rëndësishëm në zhvillimin dhe përshtatjen e metodologjisë së *5G Toolbox*, me fokus të veçantë në adresimin e aspekteve të sigurisë kibernetike dhe në procesin e identifikimit të pajisjeve dhe komponentëve kritikë të rrjeteve. Ky kontribut ka synuar forcimin e vlerësimit të rreziqeve dhe përcaktimin e masave parandaluese për mbrojtjen e infrastrukturave të komunikimeve elektronike.

Metodologjia e zhvilluar mbështet qasjen *"secure by design",* duke integruar kërkesat e sigurisë që në fazat e hershme të projektimit, ndërtimit dhe operimit të rrjeteve 5G. Kjo qasje siguron që elementët kritikë të infrastrukturës të jenë të mbrojtur në mënyrë proaktive, duke reduktuar ekspozimin ndaj kërcënimeve kibernetike dhe duke rritur qëndrueshmërinë e përgjithshme të rrjetit.

Gjithashtu, AKEP ka kontribuar në trajtimin e kërkesave të sigurisë që lidhen me ekosistemet e ndërlidhura dhe ndërvepruese, duke marrë parasysh kompleksitetin e zinxhirit të furnizimit, ndërveprimin me rrjete të tjera kritike dhe varësitë teknologjike ndërsektoriale. Në këtë kuadër, janë adresuar elementë të tillë si menaxhimi i rrezikut, kontrolli i aksesit, besueshmëria e

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

pajisjeve dhe ndërveprimi i sigurt ndërmjet sistemeve, në përputhje me standardet dhe praktikat më të mira evropiane.

Qendra Kundër Ekstremizmit të Dhunshëm (QKEDH)

Gjatë periudhës raportuese, Qendra Kundër Ekstremizmit të Dhunshëm (QKEDH) ka zbatuar një sërë aktivitetesh ndërgjegjësuese dhe trajnuese në kuadër të projekteve të financuara nga Bashkimi Evropian dhe GCERF, me fokus forcimin e qëndrueshmërisë digjitale, zhvillimin e mendimit kritik dhe parandalimin e ekstremizmit të dhunshëm në mjedisin *online*.

Aktivitetet janë orientuar si për të rinjtë ashtu edhe profesionistëve, duke synuar rritjen e aftësive për identifikimin e përmbajtjeve radikalizuese, adresimin e gjuhës së urrejtjes dhe promovimin e një diskursi të shëndetshëm *online*. Në kuadër të fushatave ndërgjegjësuese dhe trajnimeve të zhvilluara, janë përfshirë gjithsej 130 pjesëmarrës, përfshirë 89 të rinj dhe 41 profesionistë të vijës së parë.

Aktivitetet janë realizuar në formën e sesioneve informuese, trajnimeve interaktive dhe diskutimeve të hapura, të organizuara në institucione të arsimit parauniversitar dhe të arsimit të lartë, me të cilat QKEDH ka marrëveshje bashkëpunimi, duke garantuar një qasje gjithëpërfshirëse dhe të përshtatur sipas nevojave të grupeve të synuara.
Paralelisht, QKEDH ka koordinuar me partnerë lokalë dhe organizata të shoqërisë civile, me mbështetjen e GCERF, si dhe në bashkëpunim me Këshillin Ndërfetar Shqiptar, hartimin e një plani komunikimi lokal për kundërnarrativën në luftimin e radikalizmit dhe ekstremizmit të dhunshëm online. Ky plan ka përfshirë mesazhe të strukturuara për shpërndarje në rrjetet sociale dhe platformat online, të zhvilluara në konsultim me media, gazetarë dhe aktorë të vijës së parë.

Në procesin e përgatitjes së këtyre mesazheve janë angazhuar rreth 80 pjesëmarrës, ndërsa shpërndarja ka arritur rreth 800 individë. Gjithashtu, në funksion të nxitjes së tolerancës, dialogut ndërfetar dhe luftimit të gjuhës së urrejtjes, janë zhvilluar sesione online dhe aktivitete fizike me përfaqësues të komuniteteve fetare, të udhëhequra nga HEDAYAH në kuadër të një projekti të financuar nga Bashkimi Evropian.

Si pjesë e këtij procesi, janë organizuar tre aktivitete fizike me përfaqësues nga pesë institucionet zyrtare fetare në Shqipëri, gjatë të cilave janë hartuar dhe prodhuar katër materiale video për shpërndarjen e mesazheve që promovojnë harmoninë fetare, kohezionin shoqëror dhe respektin ndërkomunitar. Këto ndërhyrje kanë kontribuar në rritjen e ndërgjegjësimit, forcimin e kapaciteteve parandaluese dhe ndërtimin e bashkëpunimit ndërinstitucional dhe ndërkomunitar, duke mbështetur përpjekjet kombëtare për parandalimin e ekstremizmit të dhunshëm dhe për krijimin e një mjedisi digjital më të sigurt dhe gjithëpërfshirës.

Agjencia Shtetërore për të Drejtat dhe Mbrojtjen Fëmijës (ASHDMF)

Në zbatim të nenit 27 të ligjit nr. 18/2017 *"Për të drejtat dhe mbrojtjen e fëmijës*", ASHDMF shqyrton çdo raportim që lidhet me faqe apo materiale me përmbajtje potencialisht të paligjshme dhe/ose të dëmshme për fëmijët në internet, duke luajtur një rol kyç në identifikimin dhe referimin e rasteve të rrezikut në mjedisin digjital. Gjatë vitit 2025, ASHDMF ka evidentuar

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

gjithsej 123 raportime, kryesisht nga fëmijë dhe prindër, të lidhura me keqpërdorimin e të dhënave personale të fëmijëve në rrjetet sociale.

Këto raportime janë pranuar përmes Linjës së Këshillimit Alo 116 111 dhe janë përcjellë pranë Autoritetit Kombëtar për Sigurinë Kibernetike (AKSK), i cili, në bashkëpunim me Policinë e Shtetit, ka ndërmarrë masat përkatëse për bllokimin e faqeve apo adresave problematike, si dhe për identifikimin e autorëve dhe viktimave të përfshira. Në rastet kur viktimat janë identifikuar, ASHDMF ka referuar rastet pranë Punonjësve për Mbrojtjen e Fëmijës (PMF), përkatës për menaxhim në terren dhe marrjen në mbrojtje të fëmijëve, në përputhje me procedurat e përcaktuara në vendimin e Këshillit të Ministrave nr. 578, datë 03.10.2018.

Gjatë vitit 2025, PMF-të kanë menaxhuar gjithsej 21 raste të identifikuara të dhunës në mjedisin digjital, përfshirë raste të shantazhimit dhe kërcënimit, publikimit të materialeve intime apo të papërshtatshme, hapjes së profileve false në rrjetet sociale, si dhe bullizimit dhe ofendimeve *online* në platforma të ndryshme digjitale.

Në të gjitha rastet e identifikuara ose të referuara nga institucionet, fëmijët apo prindërit, Punonjësit për Mbrojtjen e Fëmijës kanë kryer vlerësimin e situatës, kanë mbledhur Grupet Teknike Ndërinstitucionale (GTN) në nivel vendor dhe kanë hartuar Plane Individuale të Mbrojtjes për çdo fëmijë. GTN-të janë përbërë nga profesionistë të strukturave vendore të policisë, arsimit, shëndetësisë dhe shërbimeve sociale, duke garantuar një qasje të koordinuar dhe gjithëpërfshirëse në menaxhimin e rasteve. Paralelisht me trajtimin e rasteve, ASHDMF në bashkëpunim me institucionet përgjegjëse dhe partnerët që punojnë për mbrojtjen e fëmijëve ka realizuar 24 aktivitete ndërgjegjësuese dhe informuese, workshope, lidhur me çështjet e sigurisë në internet të fëmijëve dhe të rinjve, luftën kundër gjuhës së urrejtjes dhe radikalizimit.

Në bashkëpunim më Ministrinë e Shëndetësisë dhe Mirëqenies Sociale dhe me CRCA Shqipëri ASHDMF është bërë pjesë e Fushatës Globale "Internet i Sigurt për të Gjithë" (SID) e mbështetetur nga Bashkimi Europian së bashku me Better Internet for Kids në BE. ASHDMF është bërë pjesë e takimeve dhe aktiviteteve në kuadër të kësaj fushate, siç ishte “Forumi i 10-të Kombëtar: “Së Bashku kundër Bullizmit dhe Gjuhës së Urrejtjes në Hapësirën Kibernetike”, të zhvilluar në kuadër të Ditës Ndërkombëtare për Internet të Sigurt si dhe të gjithë veprimtarisë online në këtë fushatë.

ASHDMF ka zhvilluar aktivitete të tjera ndërgjegjësuese në bashkëpunim me AKSK:

- 12 aktivitete nga të cilat, 9 kanë qenë takime ndërgjegjësuese në shkolla 9-vjeçare dhe të mesme me pjesëmarrjen e rreth 370 fëmijëve dhe profesionistëve, nxënëns, mësues, punonjës psikosocialë, oficerë sigurie në shkolla.
- Ka koordinuar organizimin e një trajnimi të ofruar nga ekspertë të AKSK për sigurinë kibernetike për fëmijët me pjesëmarrjen e 48 PMF; 18 PMF nga bashkia Tiranë dhe 30 Njësi të Mbrojtjes së Fëmijëve nga bashkitë e tjera të vendit.
- Ka zhvilluar një tryezë të rrumbullakët mbi mbrojtjen e fëmijëve online, ku morën pjesë rreth 35 profesionistë.
- 12 aktivitete ndërgjegjësuese dhe informuese janë zhvilluar në shkolla 9-vjeçare dhe të mesme në bashkëpunim të ngushtë me NJMF-të, me drejtoritë arsimore në bashkitë Tiranë, Has, Himarë, Lezhë, Shkodër, Gjirokastër, Devoll, Memaliaj, Këlcyrë, Korçë.

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

Në takime kanë marrë pjesë edhe profesionistët e vijës së parë, NJMF/PMF mësues, stafet psikosocialë në shkolla, drejtues shkollash, oficerët e sigurisë, punonjës të policisë.

Të dhënat në shifra për pjesëmarrësit:

- Janë ndërgjegjësuar 750 fëmijë dhe të rinj;
- 210 profesionisë (drejtues shkollash, mësues, punonjës psikosocialë në shkolla, oficerë sigurie).

Fëmijët dhe profesionistët janë informuar për mënyrat e raportimit të rasteve të bullizmit, ngacmimeve, shantazheve online për fëmijët dhe të rinjtë, si dhe janë informuar mbi praktikat më të mira bashkëkohore për lundrim të sigurt në internet.

QËLLIMI I POLITIKËS 2

MBROJTJA ONLINE E QYTETARËVE DHE NXITJA E KULTURËS KIBERNETIKE

Kjo politikë synon të forcojë mbrojtjen *online* të qytetarëve dhe të promovojë një kulturë të qëndrueshme kibernetike në Shqipëri. Ajo fokusohet në përmirësimin e kuadrit ligjor, rritjen e ndërgjegjësimit dhe zhvillimin e aftësive kibernetike për të gjithë qytetarët, përfshirë grupet e nënpërfaqësuara.

Përmes dialogut ndërinstitucional, aktiviteteve ndërgjegjësuese dhe programeve edukative, politika synon ndërtimin e një ekosistemi të fortë dhe të qëndrueshëm të sigurisë kibernetike, që garanton pjesëmarrje të barabartë dhe mbrojtje efektive në hapësirën digjitale.

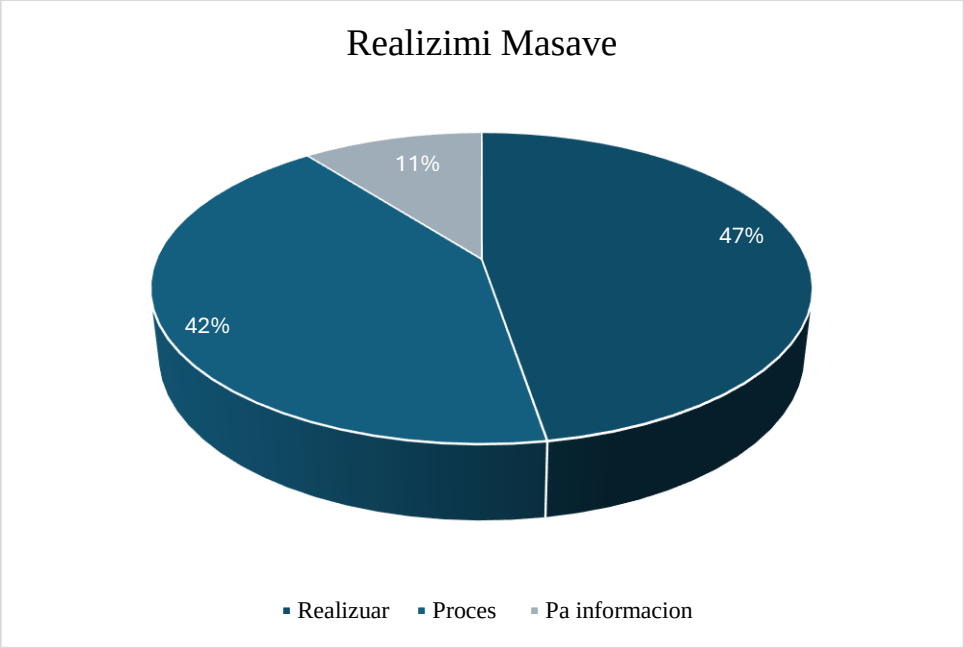
Objektivat e politikës fokusohen në:

- Hartimin dhe zhvillimin e Planit Kombëtar për Ndërgjegjësimin e Qytetarëve (PKNQ);
- Hartimin e një kornize ligjore për qasjen gjithëpërfshirëse të qytetarëve;
- Krijimi i mekanizmave të nevojshëm për mbrojtjen *online* të fëmijëve;
- Nxitja e barazisë gjinore në hapësirën digjitale;
- Krijimi i mekanizmave të duhur për mbrojtjen e SME-ve *online*;
- Krijimi i mekanizmave të nevojshëm për mbrojtjen dhe fuqizimin e grupeve të nënpërfaqësuara.

Gjatë vitit 2025, Plani i Veprimit 2025-2027, për Politikën 2, parashikon zbatimin e gjithsej 19 masave. Nga të cilat, siç vërehet edhe nga Grafiku 3:

- 47% e Masave janë realizuar plotësisht;
- 42% e Masave janë në proces;
- 11% e Masave nuk disponohet informacion.

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



Grafiku 3. Realizimi i masave për Politikën 2

Përsa i përket përmbushjes së Objektivave Specifikë të kësaj Politike:

- **Objektivi specifik 2.1**: Synon hartimin dhe zbatimin e *Planit Kombëtar për Ndërgjegjësimin e Qytetarëve* (PKNQ), përmes analizimit të situatës aktuale të fushatave ekzistuese, identifikimit të nevojave për përmirësim dhe zhvillimit të programeve të qëndrueshme të trajnimit të segmentuar sipas grupeve të interesit. Ky objektiv përfshin përgatitjen dhe shpërndarjen e materialeve edukative të aksesueshme dhe miqësore për qytetarët dhe fëmijët, zhvillimin e fushatave të gjera ndërgjegjësuese në media, si dhe promovimin e përdorimit të mekanizmit *"RED BUTTON"* për raportimin e përmbajtjeve të paligjshme në internet;

- **Objektivi specifik 2.2:** Synon hartimin e një kornize ligjore gjithëpërfshirëse për mbrojtjen *online* të qytetarëve, përmes analizimit dhe identifikimit të nevojës për ndryshime në legjislacionin ekzistues, me qëllim forcimin e sigurisë së tyre në hapësirën digjitale. Ky objektiv përfshin gjithashtu përgatitjen e një projektligji të posaçëm për mbrojtjen online të qytetarëve nga kërcënimet e mundshme kibernetike, duke garantuar një qasje të integruar, parandaluese dhe mbrojtëse;

- **Objektivi specifik 2.3:** Synon krijimin e mekanizmave të qëndrueshëm për mbrojtjen *online* të fëmijëve, përmes integrimit të sigurisë kibernetike në sistemin arsimor dhe forcimit të rolit të shkollës dhe familjes. Ky objektiv përfshin rishikimin dhe përmirësimin e kurrikulave mësimore, trajnimin e vazhdueshëm të stafit arsimor, integrimin e moduleve të dedikuara për mbrojtjen *online* të fëmijëve dhe të rinjve, si dhe realizimin e fushatave informuese për prindërit mbi përdorimin e mekanizmave të kontrollit prindëror;

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

- **Objektivi specifik 2.4:** Ka për qëllim nxitjen e barazisë gjinore në hapësirën digjitale, duke promovuar përfshirjen aktive të grave dhe vajzave në fushën e teknologjisë dhe sigurisë kibernetike. Ky objektiv realizohet përmes mbështetjes së edukimit dhe karrierës së tyre, organizimit të trajnimeve vjetore të dedikuara, si dhe zhvillimit të fushatave ndërgjegjësuese për garantimin e mundësive të barabarta në sektorin digjital;

- **Objektivi specifik 2.5**: Synon krijimin e mekanizmave të duhur për mbrojtjen *online* të Ndërmarrjeve të Vogla dhe të Mesme *(SME)*, përmes rritjes së ndërgjegjësimit dhe kapaciteteve të tyre në fushën e sigurisë kibernetike. Ky objektiv përfshin edukimin e SME-ve mbi rreziqet kibernetike, përgatitjen e udhëzimeve praktike mbi masat mbrojtëse, si dhe organizimin e trajnimeve vjetore të dedikuara për punonjësit e tyre;

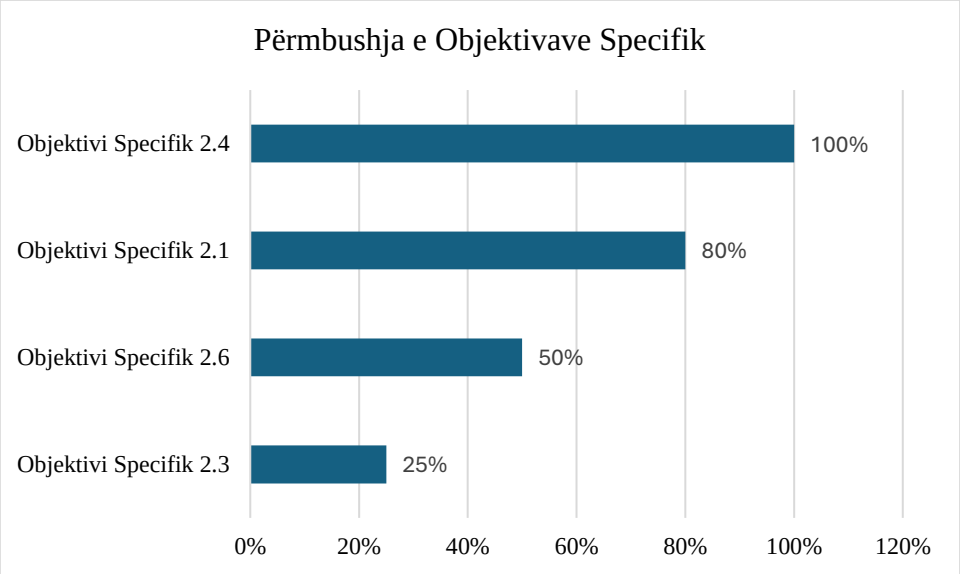
- **Objektivi specifik 2.6**: Ka si qëllim mbrojtjen dhe fuqizimin e grupeve të nënpërfaqësuara në hapësirën digjitale, përmes krijimit të mekanizmave gjithëpërfshirës dhe të aksesueshëm. Ky objektiv realizohet nëpërmjet zhvillimit të një platforme kombëtare me mjete edukative dhe interaktive për rritjen e ndërgjegjësimit mbi sigurinë *online*, si dhe hartimit dhe shpërndarjes së materialeve edukative të përshtatura sipas nevojave specifike të këtyre grupeve.

Nga analiza rezulton se:

- Objektivi Specifik 2.1 është realizuar në masën 80%
- Objektivi Specifik 2.3 është realizuar në masën 25%
- Objektivi Specifik 2.4 është realizuar në masën 100%
- Objektivi Specifik 2.6 është realizuar në masën 50%

Në lidhje me objektivat specifike 2.2 dhe 2.5, janë evidentuar rezultatet e mëposhtme:

- Objektivi Specifik 2.2 nuk është realizuar;
- Objektivi Specifik 2.5 është në proces realizimi;



Grafiku 4. Përmbushja e Objektivave Specifikë për Politikën 2

Ndër rezultatet kryesore të arritura, në kuadër të përmbushjes së masave të parashikuara në

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

Planin e Veprimit 2025-2027 të miratuar, në lidhje me Politikën 2 janë:

- Janë analizuar dhe vlerësuar aktivitetet ekzistuese ndërgjegjësuese në nivel kombëtar, me fokus sigurinë *online* të qytetarëve, fëmijëve dhe grupeve të ndryshme shoqërore, duke identifikuar nevojat për përmirësim dhe qasje më të strukturuar;
- Janë zhvilluar programe dhe sesione trajnimi të vazhdueshme, të përshtatura sipas grupeve të interesit (fëmijë, të rinj, prindër, mësues, qytetarë), me fokus kërcënimet kibernetike, *phishing*, keqpërdorimin e të dhënave personale dhe sjelljen e sigurt në internet;
- Janë përgatitur dhe shpërndarë materiale edukative të qarta, të aksesueshme dhe në gjuhë të kuptueshme, përfshirë materiale miqësore për fëmijët, mbi higjienën kibernetike, sigurinë në internet dhe mbrojtjen e të dhënave personale;
- Janë realizuar fushata informuese dhe sensibilizuese në shkolla dhe komunitete, përmes formave ndërvepruese dhe kanaleve të ndryshme të komunikimit, me synim rritjen e ndërgjegjësimit publik për sigurinë kibernetike;
- Është promovuar përdorimi i mekanizmit "*RED BUTTON*" dhe platformave të raportimit për përmbajtje të paligjshme *online*, duke rritur ndërgjegjësimin për raportimin e rasteve të bullizmit kibernetik, përmbajtjeve të dëmshme dhe shkeljeve në hapësirën digjitale;
- Ka vijuar procesi i rishikimit dhe përditësimit të kurrikulave, me integrimin e elementëve të sigurisë kibernetike dhe qytetarisë digjitale në arsimin parauniversitar;
- Janë realizuar trajnime për stafin mësimor dhe profesionistë të arsimit mbi sigurinë kibernetike, etikën digjitale dhe mbrojtjen *online* të fëmijëve, duke ngritur kapacitetet për edukim dhe parandalim në shkolla;
- Janë integruar module për sigurinë kibernetike dhe mbrojtjen *online* të fëmijëve dhe të rinjve në kurrikulat mësimore, veçanërisht në lëndën e TIK-ut, me shtrirje progresive në të gjitha nivelet;
- Janë realizuar fushata dhe takime informuese për prindërit mbi përdorimin e aplikacioneve dhe platformave të sigurisë kibernetike, përfshirë mekanizmat e kontrollit prindëror;
- Janë ndërmarrë iniciativa për promovimin e edukimit dhe karrierës së grave dhe vajzave në teknologji dhe siguri kibernetike, duke nxitur përfshirjen e tyre aktive në hapësirën digjitale;
- Janë organizuar trajnime dhe aktivitete vjetore të dedikuara për vajzat dhe gratë në fushën e sigurisë kibernetike, përfshirë aktivitete praktike dhe gara profesionale;
- Janë zhvilluar fushata sensibilizuese për promovimin e mundësive të barabarta për gratë në sektorin digjital.

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

- Analizimi i situatës aktuale lidhur me fushatat dhe programet e ndërgjegjësimit, si dhe vlerësimi i nevojave për rishikimin dhe përmirësimin e tyre;
- Rishikimi i kurrikulës së arsimit parauniversitar për evidentimin e përfshirjes së sigurisë kibernetike dhe formulimin e rekomandimeve për përmirësimet e nevojshme;

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

- Trajnimi i stafit mësimor mbi sigurinë kibernetike dhe hartimi i një programi të rregullt dhe të qëndrueshëm për ngritjen e kapaciteteve në shkolla;
- Integrimi i moduleve për sigurinë kibernetike dhe mbrojtjen *online* të fëmijëve dhe të rinjve në kurrikulat mësimore në të gjitha nivelet e arsimit;
- Promovimi i edukimit të Ndërmarrjeve të Vogla dhe të Mesme (SME) në fushën e teknologjisë dhe sigurisë kibernetike;
- Përgatitja e udhëzimeve praktike mbi masat e sigurisë kibernetike për Ndërmarrjet e Vogla dhe të Mesme (*SME*);
- Organizimi i trajnimeve vjetore të dedikuara për punonjësit e SME-ve;
- Krijimi i një platforme kombëtare me mjete edukative dhe interaktive për rritjen e ndërgjegjësimit mbi sigurinë *online* për qytetarët dhe grupet e interesit.

INFORMACION MBI ZBATIMIN E MASAVE

Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK)

Ka siguruar zbatimin e Politikës 2 , duke udhëhequr dhe harmonizuar aktivitete ndërgjegjësuese, edukative dhe mekanizma raportimi për mbrojtjen *online* të qytetarëve dhe forcimin e kulturës së sigurisë kibernetike. Gjatë vitit 2025, AKSK ka organizuar gjithsej 21 aktivitete ndërgjegjësuese të dedikuara për fëmijët, të zhvilluara në disa qytete të vendit, në bashkëpunim të ngushtë me ASHDMF dhe partnerë të shoqërisë civile.

Këto aktivitete kanë pasur në fokus përdorimin e sigurt dhe të përgjegjshëm të internetit, parandalimin e rreziqeve digjitale, si dhe rritjen e aftësive të fëmijëve për të identifikuar dhe raportuar përmbajtje të dëmshme *online*. Paralelisht, janë organizuar trajnime të posaçme për trajnerë dhe profesionistë të arsimit, me qëllim forcimin e kapaciteteve të tyre në edukimin dhe mbrojtjen *online* të fëmijëve dhe të rinjve.

Në kuadër të këtyre nismave, janë përfshirë mbi 370 fëmijë dhe profesionistë, të cilët janë trajnuar mbi temat e sigurisë në internet, mbrojtjes nga përmbajtjet e dëmshme, sjelljes etike në hapësirën digjitale dhe përdorimit të mekanizmave të raportimit *online*, duke kontribuar në ndërtimin e një qasjeje parandaluese dhe të qëndrueshme ndaj rreziqeve kibernetike. Në kuadër të Objektivit 2.1, AKSK ka vijuar të promovojë në mënyrë aktive përdorimin e mekanizmave zyrtarë për raportimin e përmbajtjeve të paligjshme online, përfshirë mekanizmin "*RED BUTTON*" dhe "Raporto", si pjesë e përpjekjeve për forcimin e kulturës së raportimit dhe reagimit institucional.

Gjatë periudhës janar-dhjetor 2025, në këto mekanizma janë regjistruar 225 raportime, të lidhura kryesisht me raste të bullizmit kibernetik, profile të rreme dhe përhapje të përmbajtjeve të papërshtatshme. Të gjitha rastet e raportuara janë referuar për trajtim të mëtejshëm pranë institucioneve kompetente, duke garantuar një zinxhir të koordinuar reagimi dhe mbrojtjeje për qytetarët. Gjithashtu, AKSK ka dhënë një kontribut të rëndësishëm në nxitjen e barazisë gjinore dhe përfshirjes sociale në hapësirën digjitale, përmes organizimit të Maratonës Kombëtare për Vajzat dhe Gratë në Sigurinë Kibernetike, si dhe Maratonës Speciale për grupet e nënpërfaqësuara. Këto iniciativa kanë shërbyer si modele praktike të qasjes gjithëpërfshirëse në edukimin digjital, duke krijuar mundësi të barabarta për zhvillimin e aftësive kibernetike, rritjen e vetëbesimit dhe përfshirjen aktive të grupeve të nënpërfaqësuara në ekosistemin kombëtar të sigurisë kibernetike.

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

Qendra Kundër Ekstremizmit të Dhunshëm (QKEDH)

QKEDH ka kontribuar në promovimin e mekanizmave të raportimit dhe rritjen e ndërgjegjësimit mbi sigurinë *online*, veçanërisht në kontekstin e parandalimit të radikalizimit dhe ekstremizmit të dhunshëm në mjedisin digjital.

Në zbatim të Masës 2.1.5 – Promovimi për rritjen e përdorimit të "*RED BUTTON*" për raportimin e përmbajtjeve të paligjshme, QKEDH, në kuadër të projektit *READY*, ka realizuar 6 trajnime gjatë muajve nëntor–dhjetor, të fokusuara në fuqizimin e të rinjve dhe ngritjen e kapaciteteve të profesionistëve të shkollave për identifikimin dhe parandalimin e radikalizimit dhe ekstremizmit të dhunshëm në mjediset digjitale. Trajnimet janë shoqëruar me sesione ndërgjegjësimi mbi sigurinë *online* dhe mekanizmat e raportimit, përfshirë përdorimin e "*RED BUTTON*" . Këto trajnime janë zhvilluar në shkolla të arsimit parauniversitar dhe universitete, duke përfshirë nxënës, studentë dhe staf pedagogjik/akademik, si pjesë e një qasjeje parandaluese që synon rritjen e kulturës së raportimit dhe reagimit të hershëm ndaj përmbajtjeve të paligjshme dhe të dëmshme *online*.

QËLLIMI I POLITIKËS 3

FORCIMI I BASHKËPUNIMIT NDËRKOMBËTAR

Kjo politikë synon të forcojë pozicionin e vendit në ekosistemin ndërkombëtar të sigurisë kibernetike përmes harmonizimit të kuadrit ligjor, thellimit të bashkëpunimit rajonal dhe ndërkombëtar, si dhe zhvillimit të diplomacisë kibernetike. Kjo politikë adreson nevojën për përafrim të qëndrueshëm me standardet dhe praktikat ndërkombëtare, duke garantuar që politikat dhe legjislacioni kombëtar të jenë në linjë me direktivat përkatëse dhe të zbatueshme në mënyrë efektive nga autoritetet publike dhe sektori privat.

Në kuadër të harmonizimit të politikave dhe legjislacionit, parashikohet ngritja e mekanizmave të strukturuar analitikë për rishikimin dhe përmirësimin e kuadrit ligjor ekzistues, si dhe zhvillimi i fushatave ndërgjegjësuese për rritjen e nivelit të kuptimit dhe zbatimit praktik të kërkesave ligjore në fushën e sigurisë kibernetike. Këto masa synojnë të krijojnë një bazë të qëndrueshme institucionale dhe ligjore, të krahasueshme me standardet ndërkombëtare.

Gjithashtu theksohet forcimi i bashkëpunimit rajonal, veçanërisht në kuadër të WB6, dhe bashkëpunimin ndërkombëtar përmes programeve të përbashkëta të trajnimit, simulimeve dhe shkëmbimit të praktikave më të mira. Këto iniciativa synojnë rritjen e gatishmërisë kolektive ndaj incidenteve kibernetike, ndërtimin e besimit ndërinstitucional dhe përmirësimin e kapaciteteve teknike e operacionale në nivel rajonal.

Së fundi, zhvillimi i diplomacisë kibernetike përbën një shtyllë kyçe të kësaj politike, duke synuar përcaktimin e qartë të prioriteteve dhe partnerëve strategjikë, pjesëmarrjen aktive në mekanizma ndërkombëtarë dhe ndërtimin e kapaciteteve kombëtare për përfaqësim dhe negociim në fushën e sigurisë kibernetike. Në tërësi, Politika 3 kontribuon në rritjen e rolit dhe besueshmërisë së vendit si partner aktiv dhe i përgjegjshëm në arkitekturën ndërkombëtare të sigurisë kibernetike.

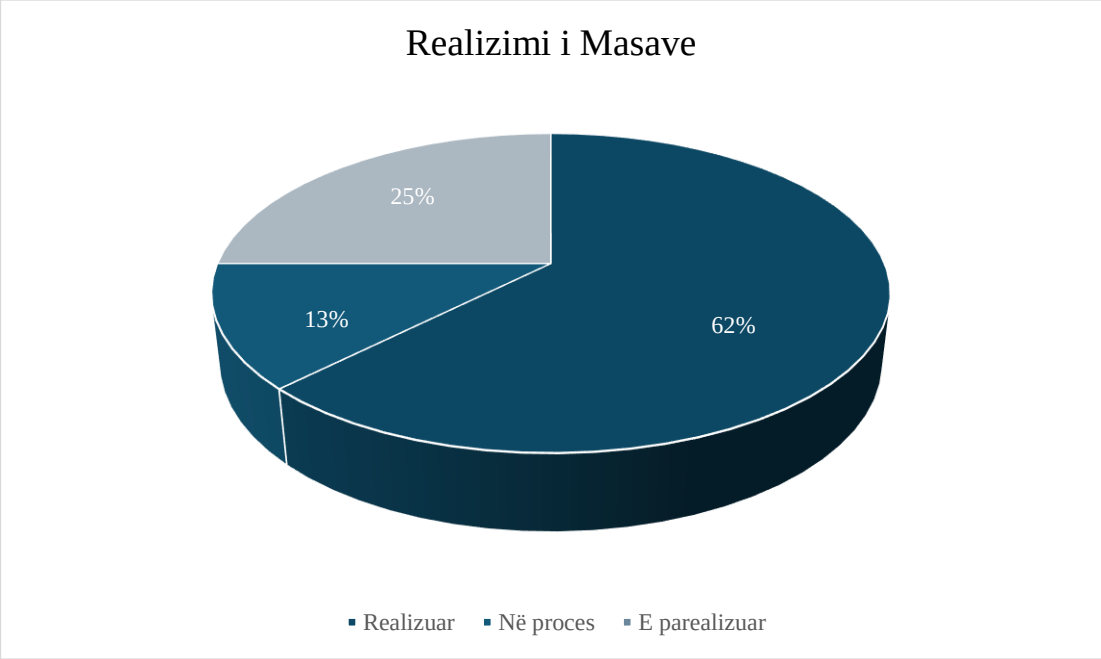
Adresa: Rruga "Papa Gjon Pali II", Nr. 3, Kati 1, Tiranë
Faqe web: www.aksk.gov.al | E-mail: info@aksk.gov.al
Tel./Fax: 04 2221 039

Objektivat e Politikës 3 fokusohen në:

- Objektivi specifik 3.1: Harmonizimi i Politikave dhe Legjislacionit ;
- Objektivi specifik 3.2: Forcimi i Bashkëpunimit Rajonal (WB6) dhe Ndërkombëtar;
- Objektivi specifik 3.3: Zhvillimi i Diplomacisë Kibernetike .

Gjatë vitit 2025, Plani i Veprimit për Politikën 3 parashikon zbatimin e gjithsej shtatë masave, nga të cilat:

- 62 % e Masave janë realizuar plotësisht;
- 13 % e Masave janë në proces;
- 25 % e Masave janë pa informacion.

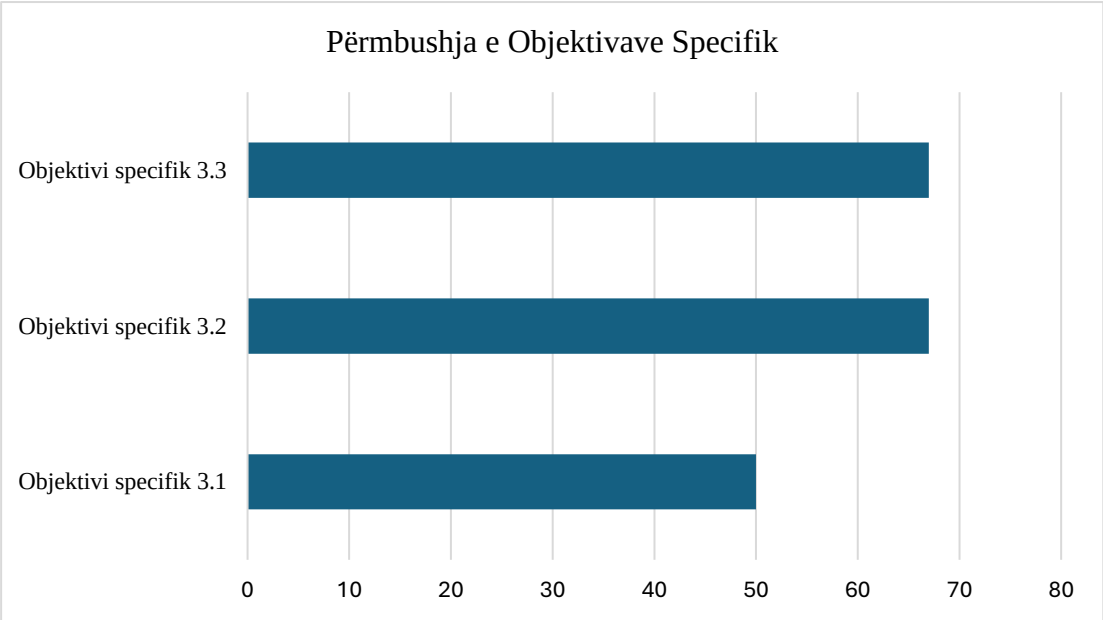


Grafiku 5. Realizimi i masave për Politikën 3

Për sa i përket përmbushjes së Objektivave Specifikë të kësaj Politike, nga analiza rezulton se:

- Objektivi specifik 3.1 është realizuar në masën 50%;
- Objektivi specifik 3.2 është realizuar në masën 67%;
- Objektivi specifik 3.3 është realizuar në masën 67%.

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



Grafiku 6. Përmbushja e Objektivave Specifikë për Politikën 3

Objektivi specifik 3.1 - Harmonizimi i politikave dhe legjislacionit synon të sigurojë përafrimin e kuadrit kombëtar të politikave dhe legjislacionit në fushën e sigurisë kibernetike me direktivat, standardet dhe praktikat më të mira ndërkombëtare. Ky objektiv fokusohet në krijimin e mekanizmave të qëndrueshëm institucionalë për analizimin dhe rishikimin e kuadrit ligjor ekzistues, me qëllim identifikimin dhe rekomandimin e ndryshimeve të nevojshme për rritjen e përputhshmërisë dhe efektivitetit të tij. Paralelisht, objektivi synon rritjen e nivelit të ndërgjegjësimit dhe kapaciteteve të autoriteteve publike dhe sektorit privat lidhur me zbatimin praktik të politikave dhe legjislacionit të sigurisë kibernetike, duke nxitur një kuptim të përbashkët dhe një zbatim më të qëndrueshëm të detyrimeve ligjore. Në këtë mënyrë, Objektivi 3.1 kontribuon në forcimin e bazës ligjore dhe institucionale për një mjedis kibernetik më të sigurt dhe të harmonizuar me standardet ndërkombëtare.

- **Objektivi specifik 3.2 - Forcimi i bashkëpunimit rajonal,** synon forcimin e bashkëpunimit rajonal dhe ndërkombëtar në fushën e sigurisë kibernetike, përmes zhvillimit të programeve të përbashkëta trajnimi, simulimeve praktike dhe shkëmbimit të eksperiencave, me qëllim rritjen e kapaciteteve dhe koordinimit ndërinstitucional.
- **Objektivi specifik 3.3 - Zhvillimi i diplomacisë kibernetike,** synon forcimin e pozicionit të Shqipërisë në arenën ndërkombëtare në fushën e sigurisë kibernetike, përmes planifikimit strategjik, pjesëmarrjes aktive në mekanizmat ndërkombëtarë dhe ngritjes së kapaciteteve kombëtare për diplomacinë kibernetike.

INFORMACION MBI ZBATIMIN E MASAVE

Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK)

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

Gjatë vitit 2025, AKSK ka ndërmarrë dhe zbatuar një sërë aktivitetesh që kanë dhënë një kontribut të drejtpërdrejtë në forcimin e bashkëpunimit rajonal dhe ndërkombëtar në fushën e sigurisë kibernetike, duke krijuar hapësira të strukturuara për dialog, shkëmbim përvojash dhe ndarje praktikash më të mira ndërmjet aktorëve përkatës.

Në këtë kuadër, më datat 6-7 Shkurt, në Tiranë u zhvillua një trajnim me *CERT of Poland and Western Balkan CERTs*", me pjesëmarrjen e 20 përfaqësuesve nga ekipet kombëtare të reagimit ndaj incidenteve kibernetike, ku u mundësua shkëmbimi i përvojave dhe praktikave më të mira mbi menaxhimin e incidenteve.

Më datat 10-11 Shkurt 2025**,** u zhvillua konferenca me tematikë "Rritja e Bashkëpunimit për Sigurinë Kibernetike në Evropën Juglindore - SEECP", e cila shërbeu si një forum i rëndësishëm politik dhe institucional për thellimin e bashkëpunimit ndërmjet 13 shteteve pjesëmarrëse.

Më datat 9-10 Tetor 2025**,** u zhvillua në Tiranë, Konferenca e NATO-s për Mbrojtjen Kibernetike, një ndër aktivitetet më të rëndësishme të vitit, e cila shërbeu si një platformë e nivelit të lartë për ndarjen e praktikave më të mira, forcimin e bashkëpunimit euroatlantik dhe adresimin e kërcënimeve hibride. Realizimi i kësaj konference kontribuoi ndjeshëm në rritjen e rolit të Shqipërisë si partner aktiv dhe i besueshëm në ekosistemin ndërkombëtar të sigurisë kibernetike, si dhe në zhvillimin e diplomacisë kibernetike.

Gjithashtu, më datat 16-17 Tetor 2025, u zhvillua tryeza rajonale "*Western Balkans Cyber Policy Dialogue*", e cila u fokusua në harmonizimin e politikave kombëtare të sigurisë kibernetike me direktivat e Bashkimit Evropian dhe në forcimin e mekanizmave të koordinimit ndërinstitucional. Ky aktivitet kontribuoi njëkohësisht në objektivin e forcimit të bashkëpunimit rajonal dhe në nxitjen e harmonizimit të politikave, duke krijuar baza për një qasje më të unifikuar rajonale.

Më 16 dhjetor 2025 u zhvillua një takim me donatorët dhe partnerët ndërkombëtarë, që shërbeu si një platformë strategjike për forcimin e bashkëpunimit ndërkombëtar dhe koordinimin e mbështetjes për iniciativat prioritare në fushën e sigurisë kibernetike. Prezantimi i projekteve dhe vizionit strategjik kontribuoi në forcimin e pozicionimin të Shqipërisë si aktor me rol proaktiv në ndërtimin e qëndrueshmërisë kibernetike kombëtare dhe rajonale.

Ministria për Evropën dhe Punët e Jashtme (MEPJ)

I ka kushtuar një vëmendje të veçantë forcimit të bashkëpunimit rajonal në fushën e sigurisë kibernetike, duke e konsideruar atë një prioritet të politikës së jashtme në fushën e mbrojtjes. Në këtë drejtim, janë mbështetur dhe promovuar iniciativa që synojnë hartimin e programeve rajonale për trajnime dhe simulime të përbashkëta mbi sulmet kibernetike, me qëllim rritjen e gatishmërisë dhe reagimit të koordinuar ndaj kërcënimeve në nivel rajonal.

MEPJ ka marrë pjesë në takimet dhe aktivitetet e organizuara nga Qendra e Kapaciteteve Kibernetike të Ballkanit Perëndimor (WB3C), veçanërisht në nismat e dedikuara për diplomacinë kibernetike dhe forcimin e kapaciteteve kombëtare në këtë fushë. Në këtë kuadër, janë propozuar edhe mundësi konkrete bashkëpunimi për vitin 2026, përfshirë zhvillimin e trajnimeve dhe simulimeve të përbashkëta në funksion të diplomacisë kibernetike. Paralelisht, në bashkëpunim

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

me Francën dhe Sllovenинë, si bashkëthemeluese të WB3C, MEPJ ka negociuar, lehtësuar dhe koordinuar procesin e anëtarësimit të Republikës së Shqipërisë në këtë qendër.
Gjatë vitit 2025, MEPJ mori pjesë në Rrjetin e Diplomacisë Kibernetike në Ballkanin Perëndimor, një nismë e iniciuar nga Ministria e Jashtme Gjermane dhe e implementuar përmes GIZ. Kjo nismë synon krijimin e një rrjeti të qëndrueshëm rajonal për bashkëpunim në fushën e diplomacisë kibernetike, duke përfshirë edhe trajnimin e diplomatëve në këtë fushë. Në kuadër të këtij rrjeti, është propozuar, ndër të tjera, hartimi i një Udhërrëfyesi për forcimin e strategjive rajonale dhe bashkëpunimin me sektorin privat dhe botën akademike, ku MEPJ do të kontribuojë në mënyrë aktive.

Në bashkëpunim me zyrën e Qendrës së Gjenevës për Qeverisjen e Sektorit të Sigurisë (DCAF) në Tiranë, MEPJ ka nisur negociatat për hartimin e një plani aktivitetesh të fokusuara në kërcënimet hibride, të adresuara për diplomatët dhe zyrtarët përgjegjës për çështjet e sigurisë. Ky bashkëpunim synon ngritjen e kapaciteteve institucionale dhe rritjen e ndërgjegjësimit mbi sfidat e reja të sigurisë në një mjedis gjithnjë e më kompleks.

Gjatë vitit 2025, një rëndësi e veçantë i është kushtuar edhe organizimit të konferencave dhe aktiviteteve në vend me aktorë ndërkombëtarë në fushën e diplomacisë kibernetike. Në këtë kuadër, MEPJ, në bashkëpunim me Qendrën për Bashkëpunimin Ndërkombëtar Ligjor të Holandës (CILC), Akademinë Estoneze për Bashkëqeverisje (eGA) dhe Agjencinë Çeke për Sigurinë e Informacionit (NUKIB), në kuadër të projektit të Bashkimit Evropian për Sigurinë Kibernetike për Ballkanin Perëndimor, organizoi më 13 tetor 2025 Takimin Online me Rrjetin e Ambasadorëve Shqiptarë mbi Diplomacinë Kibernetike. Ky takim, i pari i këtij formati, kishte si qëllim brifimin mbi zhvillimet e fundit, sfidat dhe praktikat më të mira në këtë fushë, si dhe rritjen e ndërgjegjësimit të rrjetit diplomatik mbi rolin strategjik të diplomacisë kibernetike në sigurinë kombëtare.

Në vijim të këtyre përpjekjeve, më 2 Qershor 2025, MEPJ, në bashkëpunim me projektin e BE-së *Cyber Balkans* dhe CILC, organizoi "Konferencën për Diplomacinë Kibernetike", e para e këtij lloji për institucionin. Konferenca u zhvillua në funksion të thellimit të bashkëpunimit me partnerët ndërkombëtarë dhe synoi rritjen e kapaciteteve dhe ndërgjegjësimit, si brenda MEPJ-së ashtu edhe në institucionet dhe agjencitë e tjera të Republikës së Shqipërisë, mbi trajtimin e çështjeve të sigurisë kibernetike dhe rolin e diplomacisë në këtë fushë.

Në aspektin e bashkëpunimit ndërinstitucional dhe ndërkombëtar, në qershor 2025 MEPJ nënshkroi një Memorandum Mirëkuptimi me Autoritetin Kombëtar për Sigurinë Kibernetike (AKSK), me qëllim forcimin e bashkëpunimit institucional në fushën e mbrojtjes kibernetike.

Po ashtu, në nëntor 2025, në kuadër të bashkëpunimit qeveri-me-qeveri me Italinë, u nënshkrua një Memorandum Mirëkuptimi për thellimin e bashkëpunimit kibernetik. Për vitin 2026, MEPJ ka parashikuar zgjerimin e këtij bashkëpunimi përmes nënshkrimit të marrëveshjeve të ngjashme me vende të tjera, veçanërisht në fushën e kërcënimeve hibride dhe kibernetike. Në këtë kuadër, është konfirmuar nënshkrimi i një Memorandumi Mirëkuptimi me Poloninë, si dhe po eksplorohen mundësi bashkëpunimi me partnerë të tjerë evropianë.

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

Gjithashtu, në përmbushje të obligimeve dhe përgjegjësive institucionale, MEPJ është bërë pjesë e Ekipit të Përgjigjes ndaj Emergjencave dhe Krizave të Sigurisë Kibernetike (CERT), duke kontribuar në mekanizmat kombëtarë të koordinimit dhe reagimit ndaj incidenteve kibernetike.

Gjatë periudhës raportuese, Politika 3 ka shënuar një nivel realizimi prej 63%**,** bazuar në progresin e masave të zbatuara.

QËLLIMI I POLITIKËS 4

NXITJA E INOVACIONIT DHE KËRKIMIT SHKENCOR NË SIGURINË KIBERNETIKE

Kjo politikë synon të krijojë një ekosistem të qëndrueshëm inovacioni dhe kërkimi shkencor në fushën e sigurisë kibernetike, duke forcuar bashkëpunimin ndërmjet institucioneve publike, universiteteve, qendrave kërkimore dhe sektorit privat. Kjo politikë fokusohet në zhvillimin e kapaciteteve kombëtare për kërkim, inovacion dhe transferim të njohurive, me qëllim adresimin proaktiv të kërcënimeve kibernetike dhe rritjen e qëndrueshmërisë digjitale të vendit.
Përmes mbështetjes së projekteve kërkimore, nxitjes së teknologjive të reja, promovimit të *startup*-eve dhe përfshirjes aktive në programe rajonale dhe evropiane të kërkimit dhe inovacionit, Politika 4 kontribuon drejtpërdrejt në forcimin e sovranitetit digjital dhe zhvillimin ekonomik. Zbatimi i saj synon ta pozicionojë sigurinë kibernetike si një fushë strategjike të zhvillimit afatgjatë, duke krijuar vlerë të shtuar për institucionet, bizneset dhe shoqërinë në tërësi.

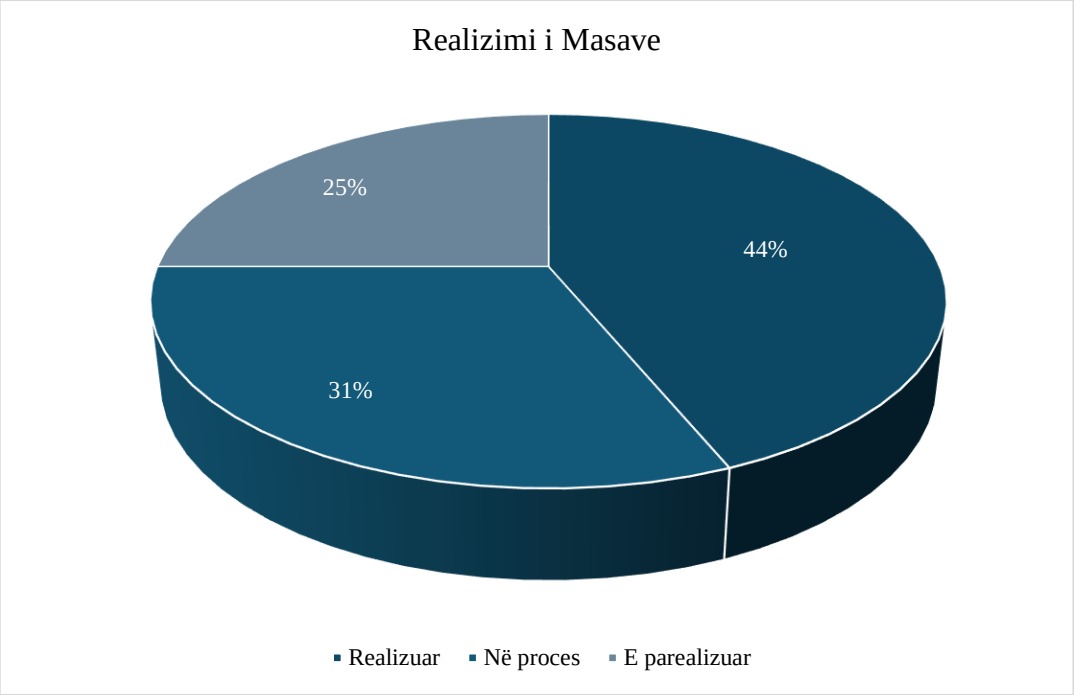
Objektivat e Politikës 4 fokusohen në:

- **Objektivi 4.1** : Ngritja e Qendrës Kombëtare të Ekselencës për Sigurinë Kibernetike;
- **Objektivi 4.2** : Mbështetja e Startup-eve në fushën e Sigurisë Kibernetike;
- **Objektivi 4.3** : Zhvillimi i Programeve të Financimit për Kërkim dhe Inovacion në Sigurinë Kibernetike.

Gjatë vitit 2025, Plani i Veprimit për Politikën 4 parashikon zbatimin e gjithsej 16 masave, nga të cilat:

- 44 % e Masave janë realizuar plotësisht;
- 31 % e Masave janë në proces;
- 25 % e Masave nuk janë realizuar.

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



Grafiku 7. Realizimi i masave për Politikën 4

Për sa i përket përmbushjes së Objektivave Specifikë të kësaj Politike, nga analiza rezulton se:

- Objektivi 4.2 është realizuar në masën 100 %

Rezulton se Objektivi 4.1 nuk ka shënuar masa të realizuara gjatë periudhës së raportimit, për shkak të natyrës përgatitore dhe varësisë nga procese të mëtejshme institucionale dhe ndërinstitucionale.
Objektivi 4.2 është realizuar në masën 100%, pasi të gjitha masat e parashikuara në kuadër të këtij objektivi janë zbatuar ose janë në zbatim të vazhdueshëm, duke kontribuar drejtpërdrejt në nxitjen e inovacionit dhe mbështetjen e ekosistemit të *startup* -eve në fushën e teknologjisë së informacionit dhe sigurisë kibernetike.
Objektivi 4.3 nuk ka shënuar masa të realizuara gjatë kësaj periudhe raportimi, pasi masat përkatëse ndodhen në fazë konceptimi, koordinimi ose përgatitore dhe nuk kanë arritur ende fazën e zbatimit operacional.

INFORMACION MBI ZBATIMIN E MASAVE

Ministria e Ekonomisë dhe Inovacionit (MEI)
Lidhur me Objektivin 4.1 - Ngritja e Qendrës Kombëtare të Ekselencës për Sigurinë Kibernetike ka raportuar se ndodhet në pritje të shkresës zyrtare nga Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK), me qëllim formalizimin e përfshirjes së saj në kuadër të bashkëpunimit ndërinstitucional dhe dhënies së kontributit për hartimin dhe miratimin e kuadrit rregullator për ngritjen dhe funksionimin e Qendrës Kombëtare për Ekselencë në Sigurinë Kibernetike (QKESK).

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

Zbatimi i Masës 4.1.2, që synon krijimin e mekanizmave për monitorimin dhe vlerësimin e performancës së QKESK, rezulton i ndërlidhur drejtpërdrejt me miratimin e kuadrit rregullator dhe institucional të parashikuar në Masën 4.1.1. Për këtë arsye, gjatë periudhës së raportimit nuk janë evidentuar zhvillime konkrete në drejtim të hartimit apo zbatimit të mekanizmave të monitorimit dhe vlerësimit të performancës.

Në lidhje me Masën 4.1.3, e cila parashikon pajisjen e QKESK me laboratorë kërkimorë dhe infrastrukturë për testimin e teknologjive të reja, realizimi i saj mbetet i kushtëzuar nga krijimi formal dhe funksional i QKESK, si dhe nga përcaktimi i qartë i rolit, mandatit dhe strukturës organizative të saj. Gjatë periudhës së raportimit, kjo masë nuk ka shënuar progres operacional, për shkak të varësisë së drejtpërdrejtë nga zbatimi i Masës 4.1.1.

Në kuadër të Masës 4.1.4, është raportuar një nismë konkrete e mbështetur nga Organizata Botërore e Pronësisë Intelektuale (WIPO), e cila synon forcimin e bashkëpunimit ndërmjet institucioneve kërkimore, universiteteve teknike, *startup* -eve dhe industrisë. Konkretisht, WIPO ka hartuar një raport vlerësimi për situatën aktuale në Republikën e Shqipërisë lidhur me krijimin e një Zyre për Transferimin e Teknologjisë (TTO) në një nga universitetet teknike të vendit.

Në kuadër të këtij projekti, janë zhvilluar tre workshope *online* me përfaqësues të universiteteve, Ministrisë së Arsimit dhe Drejtorisë së Përgjithshme të Pronësisë Industriale (DPPI). Projekti synon të kontribuojë në komercializimin efektiv të pronës intelektuale dhe në forcimin e ekosistemit të inovacionit. Masa konsiderohet në proces, me vijimësi të parashikuar gjatë vitit 2026, në varësi të ekspertizës së mëtejshme që do të ofrohet nga WIPO.

Zbatimi i Masës 4.1.5, që synon nxitjen dhe promovimin e shkëmbimit të njohurive dhe eksperiencave mbi zgjidhjet inovative në fushën e sigurisë kibernetike, rezulton i ndërlidhur ngushtësisht me ngritjen dhe funksionimin operacional të QKESK. Gjatë periudhës së raportimit, për shkak të mosfinalizimit të kuadrit rregullator dhe institucional të QKESK, kjo masë nuk ka shënuar progres të matshëm dhe mbetet e varur nga realizimi i Masës 4.1.1.

Lidhur me Objektivin 4.2 - Mbështetja e *startup* -eve në fushën e Sigurisë Kibernetike MEI, në përputhje me fushën e saj të veprimtarisë, ka raportuar se ofron mbështetje financiare, hapësira mbështetëse dhe shërbime mentorimi për *startup* -et, me synim nxitjen e inovacionit, zhvillimin e kapaciteteve sipërmarrëse dhe rritjen e qëndrueshmërisë së tyre në treg. Qasja e ndjekur nuk është selektive apo preferenciale për sektorë të caktuar, por përfshin të gjitha format e *startup* -eve, përfshirë edhe ato në fushën e sigurisë kibernetike, si pjesë integrale e teknologjisë së informacionit dhe ekonomisë digjitale.

MEI ka raportuar se, përmes projekteve dhe programeve të dedikuara, në veçanti përmes projektit *Digital Innovation Unit*, siguron akses në hapësira mbështetëse për *startup* -et dhe SME-të. Projekti DIU, me kohëzgjatje nga 01.01.2025 deri më 31.12.2028, synon krijimin e një hub-i të inovacionit digjital në Shqipëri, duke ndërtuar një ekosistem të qëndrueshëm dhe gjithëpërfshirës, me fokus në inteligjencën artificiale, sigurinë kibernetike dhe aftësitë digjitale të avancuara.

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

Në kuadër të Masës 4.2.3, është raportuar se projekti *Digital Innovation Unit* (DIU) ofron akses në laboratorë dhe ambiente testimi për zhvillimin dhe përmirësimin e zgjidhjeve inovative, sipas parimit *"test before invest"*. Këto laboratorë u shërbejnë *startup* -eve, SME-ve dhe ndërmarrjeve të vogla e të mesme, duke krijuar mundësi konkrete për testim praktik të ideve dhe produkteve në faza të hershme zhvillimi.

Përfshirja e *startup* -eve në projekte kërkimore realizohet nëpërmjet ekosistemit të krijuar nga programet mbështetëse të MEI dhe bashkëpunimit me institucione arsimore dhe organizata partnere. Projekti *Cyberfort*, i implementuar nga Shkolla Profesionale Kamëz për periudhën 01.01.2025–31.12.2027, kontribuon në zhvillimin e kapaciteteve kërkimore dhe testuese për SME-të dhe *startup* -et, përmes krijimit të përmbajtjeve dhe mjeteve të trajnimit të orientuara drejt nevojave reale të tregut dhe sigurisë kibernetike.

Në kuadër të kësaj mase, MEI ka raportuar se programet e saj mbështetëse, përfshirë DIU, krijojnë mundësi për rrjetëzim dhe bashkëpunim ndërmjet *start-up*-eve, SME-ve dhe kompanive të mëdha, duke synuar integrimin e zgjidhjeve inovative në ekosistemin kombëtar të teknologjisë dhe sigurisë kibernetike. Këto partneritete kontribuojnë në rritjen e shkallëzimit të produkteve dhe shërbimeve inovative dhe në forcimin e konkurrueshmërisë së tyre në tregjet kombëtare dhe ndërkombëtare.

Agjencia për *startup* -et, në koordinim me MEI, luan një rol kyç në hartimin dhe zbatimin e programeve mbështetëse për *startup* -et, duke përfshirë instrumente financimi, inkubimi dhe mentorimi. Paralelisht, Drejtoria e Përgjithshme e Pronësisë Industriale (DPPI) organizon në mënyrë periodike trajnime të dedikuara për *startup* -et dhe institucionet e arsimit të lartë, me fokus në regjistrimin e objekteve të pronësisë industriale, me mbi 10 aktivitete trajnimi në vit.

Organizimi i aktiviteteve konkurruese dhe nismave inovative realizohet në mënyrë të integruar përmes programeve të inovacionit dhe bashkëpunimit me aktorë publikë dhe privatë. Megjithëse gjatë periudhës së raportimit nuk janë raportuar *hackathon*-e specifikisht të dedikuara vetëm për sigurinë kibernetike, programet ekzistuese krijojnë hapësirë për zhvillimin e konkurseve dhe aktiviteteve të tilla, si pjesë e ekosistemit të inovacionit digjital.

Lidhur me Objektivin 4.3. - Zhvillimi i Programeve të Financimit për Kërkim dhe Inovacion në Sigurinë Kibernetike**,** MEI ka raportuar gatishmërinë e saj për të kontribuar në proceset e konceptimit, koordinimit dhe harmonizimit të programeve dhe instrumenteve financiare kombëtare, që synojnë mbështetjen e kërkimit shkencor dhe inovacionit, përfshirë edhe në fushën e sigurisë kibernetike. Ky kontribut parashikohet të realizohet përmes ofrimit të ekspertizës institucionale dhe përfshirjes në nisma të përbashkëta me aktorë të tjerë publikë përgjegjës për politikat e kërkimit dhe inovacionit.

Në lidhje me Masën 4.3.2, MEI ka raportuar se është e hapur për të kontribuar në procesin e konceptimit dhe koordinimit për krijimin e një fondi kombëtar që synon mbështetjen e kërkimeve në sigurinë kibernetike, në bashkëpunim me institucionet përgjegjëse për kërkimin shkencor dhe zhvillimin e inovacionit. Kontributi i MEI fokusohet në harmonizimin e instrumenteve financiare

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

ekzistuese dhe në mbështetjen e nismave të përbashkëta që synojnë forcimin e ekosistemit kërkimor dhe inovativ në nivel kombëtar.

Për Masën 4.3.3, MEI ka shprehur gatishmërinë për të kontribuar në lehtësimin e aksesit të aktorëve kombëtarë në fondet e Bashkimit Evropian dhe donatorëve ndërkombëtarë për kërkim dhe zhvillim. Ky kontribut parashikohet të realizohet përmes ofrimit të ekspertizës nga strukturat përkatëse të MEI, mbështetjes në ndërtimin e kapaciteteve institucionale dhe orientimit strategjik të aktorëve publikë, akademikë dhe privatë për përfshirje në programe financimi evropiane dhe ndërkombëtare.

Gjatë periudhës raportuese, Politika 4 ka shënuar një nivel realizimi prej 44 %, bazuar në progresin e masave të zbatuara.

QËLLIMI I POLITIKËS 5

MBROJTJA NDAJ KËRCËNIMEVE HIBRIDE

Kërcënimi hibrid përfshin përdorimin e një plani apo strategjie, ku aktorë të ndryshëm kombinojnë kërcënime kibernetike me sulme në fusha të tjera, si ato fizike, ekonomike dhe informative, për të arritur qëllime specifike. Ky lloj kërcënimi shfrytëzohet shpesh nga shtete apo aktorë joshtetërorë, duke përfituar nga dobësitë në sistemet teknologjike, infrastrukturore, politike dhe sociale të objektivave apo qëllimeve të synuara. Për t'u mbrojtur ndaj kërcënimeve hibride, nevojitet një qasje e integruar, që përfshin forcimin e sigurisë së infrastrukturës kritike e të rëndësishme të informacionit, përmirësimin e kapaciteteve për zbulimin dhe parandalimin e sulmeve kibernetike, si dhe një bashkëpunim të ngushtë ndërinstitucional e ndërkombëtar, përfshirë vendet aleate të NATO-s, për të siguruar një reagim të koordinuar, të shpejtë dhe efektiv.

Objektivat e politikës fokusohen në:

- 5.1.1 Rishikimi i kuadrit ligjor ekzistues për adresimin e mbrojtjes ndaj kërcënimeve hibride;
- 5.1.2 Përditësimi i strategjive ekzistuese për përputhjen me zhvillimet e reja teknologjike dhe taktikat e kërcënimeve hibride;
- 5.1.3 Krijimi i strukturave përgjegjëse për bashkëpunimin ndërinstitucional për kërcënimet hibride;
- 5.1.4 Implementimi i mekanizmave mbikëqyrës që monitorojnë pajtueshmërinë me kuadrin ligjor;
- 5.1.5 Harmonizimi i legjislacionit kombëtar me atë ndërkombëtar për të siguruar një qasje të përbashkët në luftën ndaj kërcënimeve hibride;
- 5.1.6 Ngritja e kapaciteteve për institucionet përkatëse mbi *acquis* BE;
- 5.2.1 Krijimi i një mekanizmi kombëtar për koordinimin e reagimit ndaj kërcënimeve hibride;
- 5.2.2 Zhvillimi i mekanizmave për shkëmbimin e informacionit mes institucioneve kombëtare dhe ndërkombëtare;

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

- 5.2.3 Organizimi i trajnimeve dhe ushtrimeve të përbashkëta me OIKI/OIRI për përballimin e sulmeve hibride;
- 5.2.4 Përfshirja e partneriteteve publike dhe private per monitorimin dhe reagimin ndaj kërcënimeve hibride;
- 5.2.5 Zhvillimi i një infrastrukture të dedikuar dhe të sigurt komunikimi për shkëmbimin në kohë reale të informacionit të ndjeshëm ndërmjet aktorëve kritikë të sigurisë kibernetike;
- 5.2.6 Nxitja e Marrëveshjeve të Bashkëpunimit Ndërkombëtar për mbrojtjen ndaj kërcënimeve hibride;
- 5.3.1 Implementimi i mjeteve dhe teknologjive të avancuara për monitorim dhe identifikim të hershëm të kërcënimeve hibride;
- 5.3.2 Implementimi i platformave për shkëmbimin e informacionit mbi kërcënimet hibride;
- 5.3.3 Hartimi i fushatave ndërgjegjësuese për rreziqet nga dezinformimi dhe sulmet kibernetike;
- 5.3.4 Përditësimi periodik i protokolleve të emergjencës bazuar në analizën e rreziqeve më të fundit;
- 5.3.5 Përdorimi i teknologjive të inteligjencës artificiale për analizimin e të dhënave dhe parashikimin e kërcënimeve hibride;
- 5.4.1 Forcimi i bashkëpunimit ndërinstitucional në luftën kundër krimit kibernetik;
- 5.4.2 Përmirësimi i kuadrit ligjor për t'u harmonizuar me legjislacionin dhe konventat ndërkombëtare në fushën e krimeve kibernetike.

Gjatë vitit 2025, Plani i Veprimit 2025-2027 për Politikën 5 parashikon zbatimin e gjithsej 17[2] masave, si më poshtë vijon:

- 5.2.1 Krijimi i një mekanizmi kombëtar për koordinimin e reagimit ndaj kërcënimeve hibride;
- 5.2.2 Zhvillimi i mekanizmave për shkëmbimin e informacionit mes institucioneve kombëtare dhe ndërkombëtare;
- 5.2.3 Organizimi i trajnimeve dhe ushtrimeve të përbashkëta me OIKI/OIRI për përballimin e sulmeve hibride;
- 5.2.4 Përfshirja e partneriteteve publike dhe private per monitorimin dhe reagimin ndaj kërcënimeve hibride;
- 5.2.5 Zhvillimi i një infrastrukture të dedikuar dhe të sigurt komunikimi për shkëmbimin në kohë reale të informacionit të ndjeshëm ndërmjet aktorëve kritikë të sigurisë kibernetike;
- 5.2.6 Nxitja e Marrëveshjeve të Bashkëpunimit Ndërkombëtar për mbrojtjen ndaj kërcënimeve hibride;
- 5.3.1 Implementimi i mjeteve dhe teknologjive te avancuara për monitorim dhe identifikim të hershëm të kërcënimeve hibride;
- 5.3.2 Implementimi i platformave për shkëmbimin e informacionit mbi kërcënimet hibride;

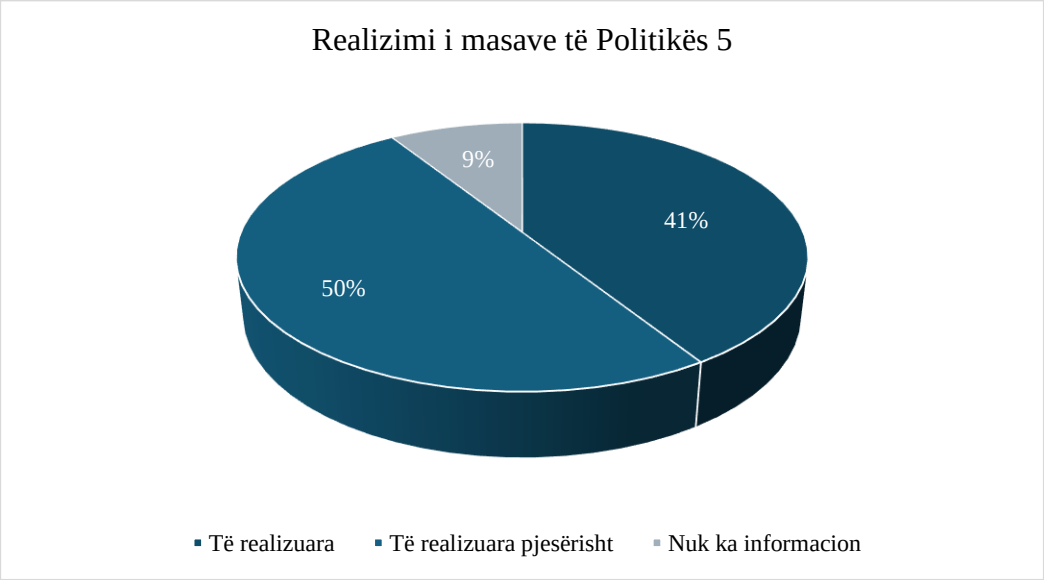
[2] *Plani i Veprimit 2025-2027 për Politikën 5 parashikon zbatimin e gjithsej 19 masave por dy prej tyre janë parashikuar për vitin 2026.*

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

- 5.3.3 Hartimi i fushatave ndërgjegjësuese për rreziqet nga dezinformimi dhe sulmet kibernetike;
- 5.3.4 Përditësimi periodik i protokolleve të emergjencës bazuar në analizën e rreziqeve më të fundit;
- 5.3.5 Përdorimi i teknologjive të inteligjencës artificiale për analizimin e të dhënave dhe parashikimin e kërcënimeve hibride;
- 5.4.1 Forcimi i bashkëpunimit ndërinstitucional në luftën kundër krimit kibernetik;
- 5.4.2 Përmirësimi i kuadrit ligjor për t'u harmonizuar me legjislacionin dhe konventat ndërkombëtare në fushen e krimeve kibernetike.

Nga të cilat:

- 41% e Masave janë realizuar plotësisht;
- 50 % e Masave janë realizuar pjesërisht;
- 9 % e Masave nuk disponohet informacion.



Grafiku 8. Realizimi i masave të Politikës 5

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

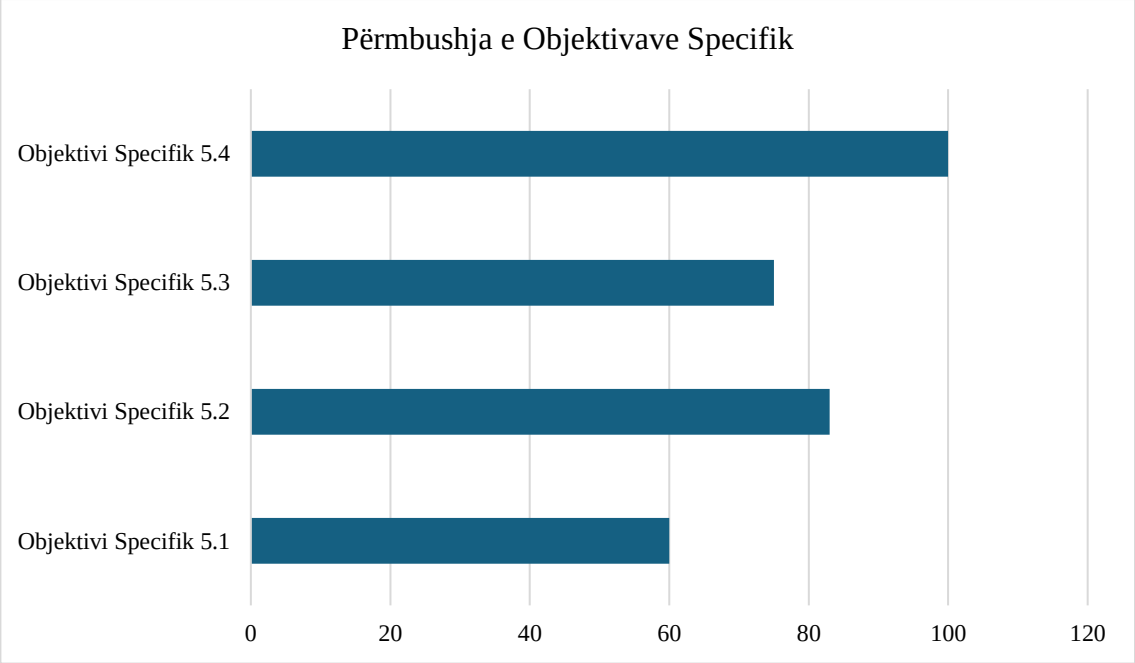
- **Objektivi Specifik 5.1**: Hartimi i Kuadrit Ligjor për Mbrojtjen ndaj Kërcënimeve Kibernetike Hibride;
- **Objektivi Specifik 5.2**: Koordinimi Ndërinstitucional dhe Ndërkombëtar;
- **Objektivi Specifik 5.3**: Krijimi i Mekanizmave të Mbrojtjes ndaj Kërcënimeve Hibride;
- **Objektivi Specifik 5.4**: Krijimi i mekanizmave për parandalimin dhe hetimin e Krimit Kibernetik.

Nga analiza rezulton se, për vitin 2025[3]:

[3] *Përllogaritur në vlerë masat e realizuara plotësisht, si dhe ato pjesërisht/progres.*

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

- Objektivi Specifik 5.1 është realizuar në masën 60 %;
- Objektivi Specifik 5.2 është realizuar në masën 83%;
- Objektivi Specifik 5.3 është realizuar në masën 75 %;
- Objektivi Specifik 5.4 është realizuar në masën 100%;



Grafiku 9. Përmbushja e Objektivave Specifik për Politikën 5

INFORMACION MBI ZBATIMIN E MASAVE

Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK)

Gjatë vitit 2025 është arritur progres i moderuar në forcimin e kapaciteteve kombëtare për adresimin e kërcënimeve hibride. Janë ndërmarrë hapa konkretë në zhvillimin e infrastrukturës teknike, përmirësimin e analizës së riskut dhe rritjen e bashkëpunimit institucional, megjithëse disa komponentë mbeten në fazë zhvillimi.

Në kuadër të masës 5.3.1 *Implementimi i mjeteve dhe teknologjive të avancuara për monitorim dhe identifikim të hershëm të kërcënimeve hibride*, implementimi i mjeteve dhe teknologjive të avancuara për monitorimin dhe identifikimin e hershëm të kërcënimeve hibride ka shënuar progres të konsiderueshëm teknik. Kapacitetet ekzistuese të monitorimit janë zgjeruar dhe përmirësuar, duke rritur aftësinë për zbulim proaktiv. Megjithatë, mbulimi ndërsektorial mbetet i pjesshëm dhe kërkon integrim më të gjerë të operatorëve të infrastrukturave kritike të informacionit.

Platforma për shkëmbimin e informacionit mbi kërcënimet hibride mbetet pjesërisht e zhvilluar. Shkëmbimi i informacionit është i konsoliduar kryesisht në dimensionin kibernetik, ndërsa nevojitet zgjerim për të përfshirë në mënyrë sistematike komponentët e tjerë të kërcënimeve hibride.

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

Lidhur me masën 5.3.2 *Implementimi i platformave për shkëmbimin e informacionit mbi kërcënimet hibride p*ërdorimi i teknologjive të inteligjencës artificiale për analizë dhe parashikim është në fazë të hershme operacionale. Iniciativat e ndërmarra gjatë vitit 2025 përfaqësojnë një bazë fillestare, por kërkojnë investime shtesë në burime njerëzore dhe kapacitete teknike për mbulim të plotë.
Organizimi i Konferencës Rajonale mbi Kërcënimet Hibride (17–21 nëntor 2025), në bashkëpunim me *Hybrid Centre of Excellence*, kontribuoi pozitivisht në rritjen e kapaciteteve institucionale dhe në forcimin e bashkëpunimit rajonal.
Paralelisht, puna për masat e mbetura si, krijimin e mekanizmave kombëtarë të koordinimit, zgjerimin e shkëmbimit ndërinstitucional të informacionit, zhvillimin e partneriteteve publike–private dhe forcimin e bashkëpunimit ndërkombëtar është në progres. Këto masa përbëjnë baza të rëndësishme për ndërtimin e një sistemi të integruar reagimi ndaj kërcënimeve hibride.

Policia e Shtetit (PSH)

Objektivi Specifik 5.1: Përmirësimi i kuadrit ligjor dhe strategjik për adresimin e kërcënimeve hibride, Policia e Shtetit ka dhënë kontribut të vazhdueshëm në rishikimin dhe përmirësimin e kuadrit ligjor që lidhet me krimin kibernetik dhe kërcënimet hibride, bazuar në përvojën praktike të strukturave hetimore dhe në standardet ndërkombëtare. Përfaqësues të Policisë së Shtetit kanë marrë pjesë aktive në takime dhe konsultime të organizuara nga Ministria e Drejtësisë, duke ofruar mendime dhe sugjerime konkrete për forcimin e dispozitave ligjore përkatëse. Gjithashtu, Policia e Shtetit është pjesë e grupit të punës për hartimin e Strategjisë kundër Krimit të Organizuar 2026–2030, ku janë reflektuar zhvillimet e reja teknologjike, format moderne të veprimtarisë kriminale, si dhe elementë që lidhen me krimin kibernetik dhe kërcënimet hibride.

Objektivi Specifik 5.2: Forcimi i bashkëpunimit dhe mekanizmave për shkëmbimin e informacionit. Në kuadër të forcimit të bashkëpunimit ndërinstitucional dhe ndërkombëtar, Policia e Shtetit ka rritur shkëmbimin e informacionit në kohë reale përmes mekanizmave të konsoliduar ligjzbatuese. Si pikë kontakti 24/7 në kuadër të Protokollit të Dytë Shtesë të Konventës së Budapestit, Policia e Shtetit siguron koordinimin operativ me institucionet kombëtare dhe partnerët ndërkombëtarë për hetimin e krimeve kibernetike dhe adresimin e kërcënimeve hibride. Njëkohësisht, është intensifikuar bashkëpunimi me institucione të tjera të sigurisë kombëtare, si dhe me partnerë ndërkombëtarë dhe rrjete të specializuara për shkëmbimin e informacionit mbi krimin kibernetik, dezinformimin dhe format e tjera të kërcënimeve hibride.

Objektivi Specifik 5.3: Rritja e kapaciteteve për parandalim, zbulim dhe reagim ndaj kërcënimeve hibride

Policia e Shtetit ka konsoliduar dhe forcuar strukturat e specializuara për analizë, monitorim dhe inteligjencë kibernetike, duke rritur aftësinë për identifikimin e hershëm të kërcënimeve hibride. Në këtë kuadër, është krijuar Sektori i Analizës, Monitorimit dhe 24/7 pranë Drejtorisë së Hetimit të Krimit Kibernetik, i cili monitoron hapësirën digjitale përmes inteligjencës kibernetike, përfshirë rrjetin e hapur, rrjetet e mbyllura dhe dark web. Janë rritur kapacitetet teknologjike përmes përdorimit të mjeteve të avancuara të analizës së burimeve të hapura (OSINT),

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

monitorimit të rrjeteve sociale dhe korelacionit të të dhënave, si dhe janë ndërmarrë hapa për modernizimin e sistemeve të informacionit dhe krijimin e bazave të integruara të të dhënave.

Paralelisht, janë zhvilluar trajnime të specializuara për punonjësit e policisë në fushat e sigurisë kibernetike, analizës së të dhënave dhe përdorimit të teknologjive bashkëkohore, duke krijuar kushtet për integrimin e platformave analitike dhe, në faza të mëtejshme, zgjidhjeve të bazuara në inteligjencë artificiale për analizë parashikuese.

Objektivi Specifik 5.4: Forcimi i bashkëpunimit ndërinstitucional dhe ndërgjegjësimit publik

Gjatë vitit 2025, Policia e Shtetit ka forcuar bashkëpunimin ndërinstitucional në luftën kundër krimit kibernetik, përfshirë nënshkrimin e marrëveshjeve të bashkëpunimit me Shoqatën e Bankave të Shqipërisë për parandalimin e mashtrimeve *online* dhe mbrojtjen e sistemeve financiare. Njëkohësisht, është intensifikuar bashkëpunimi me platformat e rrjeteve sociale për identifikimin dhe trajtimin e përmbajtjeve të paligjshme dhe veprave penale në hapësirën digjitale. Në kuadër të parandalimit, janë zhvilluar fushata ndërgjegjësuese dhe edukuese në shkolla, si dhe fushata mediatike për informimin e qytetarëve mbi rreziqet nga dezinformimi dhe sulmet kibernetike, duke kontribuar në rritjen e sigurisë publike në mjedisin *online*.

Ministria për Evropën dhe Punët e Jashtme (MEPJ)

Në kuadër të përmbushjes së Objektivit 5 për mbrojtjen ndaj kërcënimeve hibride, koordinimit ndërinstitucional dhe ndërkombëtar, veçojmë:

- Rishikimin dhe harmonizimin e kuadrit ligjor kombëtar me standardet dhe praktikat ndërkombëtare, në fushën e kërcënimeve hibride, ku MEPJ ka marrë pjesë aktive në dialogun dhe koordinimin e politikave respektive, me fokus të posaçëm bashkëpunimin me partnerë ndërkombëtarë për sigurimin e standardeve ligjore dhe teknike në sigurinë kibernetike.
- Në kuadër të hartimit dhe rishikimeve periodike të strategjive ekzistuese për t'u përshtatur me zhvillimet teknologjike dhe format e reja të kërcënimeve hibride, MEPJ ka marrë pjesë dhe kontribuar në të gjitha grupet e punës të ngritura për këtë qëllim, duke luajtur një rol thelbësor në harmonizimin e përpjekjeve kombëtare me ato ndërkombëtare, në të gjitha organizatat ndërkombëtare ku ajo është pjesë.
- Ngritja e strukturave dhe mekanizmave të bashkëpunimit ndërinstitucional dhe ndërkombëtar, për koordinimin e reagimit ndaj kërcënimeve hibride, ku MEPJ ka luajtur një rol thelbësor, me qëllim ndarjen e shpejtë të informacionit dhe kërkesës për mbështetje nga partnerët ndërkombëtar, referuar veçanërisht asistencës së NATO-s në këtë drejtim, bazuar në MoU e firmosur mes palëve AKSK-NATO.
- MEPJ koordinon raportimet dhe përfaqësimin ndërkombëtar në NATO, BE, OKB, dhe organizata të tjera ndërkombëtare ku RSH-ja është palë në fushën e mbrojtjes kibernetike. Gjithashtu merr pjesë në takime e forume kombëtare dhe ndërkombëtare në luftën kundër krimit kibernetik.
- Mbështetje dhe koordinim për harmonizim të mëtejshëm me standardet e BE-së, NATO dhe sigurimin e asisitencës ndërkombëtare, sipas rastit, në këtë drejtim.

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

MEPJ vijon koordinimin ndërinstitucional për ndarjen e informacionit dhe forcimin e kapaciteteve kombëtare në kundërveprimin ndaj kërcënimeve hibride. Gjatë këtij viti, në linjë me prioritet e politikës së jashtme shqiptare, RSH-ja ka qëndruar në solidaritet të plotë me aleatët e saj në NATO, lidhur me sulmet hibride të fundit të shoqëruara me fushata dezinformimi, dhe kontribuon në shkëmbimin dhe koordinimin e informacionit përmes mekanizmave ndërkombëtarë. Gjithashtu RSH-ja ka një politikë të qartë linjëzimi me të gjitha qëndrimet e BE-së dhe NATO-s për sigurinë kibernetike, duke synuar të kthehet në një lider rajonal në këtë drejtim.
Theksohet se, detyrat e MEPJ-së në kuadër të Strategjisë realizohen brenda buxhetit të miratuar vjetor të Ministrisë, si dhe përmes projekteve dhe programeve të mbështetura nga Bashkimi Evropian dhe partnerë të tjerë ndërkombëtarë.

Ministria e Mbrojtjes (MM)

Gjatë vitit 2025, progresi në kuadër të Objektivit 5 ka qenë i përqendruar kryesisht në bashkëpunimin ndërinstitucional, optimizimin e kapaciteteve ekzistuese teknologjike dhe forcimin e procedurave operacionale. Në drejtim të rishikimit të kuadrit ligjor (NënObjektivi 5.1.1), MM/FA ka zhvilluar bashkëpunim ndërinstitucional dhe ka kontribuar në shpërndarjen e informacionit dhe rekomandimeve për përmirësimin e kuadrit ligjor, në koordinim me AKSK. Përditësimi i strategjive ekzistuese (5.1.2) nuk ka pësuar zhvillime të reja, ndërsa mbetet në fuqi Strategjia e Mbrojtjes Kibernetike 2024–2028. Për nënobjektivat e tjera të Objektivit 5.1 nuk ka pasur ndryshime strukturore, por është vijuar bashkëpunimi teknik dhe konsultativ.

Në kuadër të koordinimit ndërinstitucional dhe ndërkombëtar (Objektivi 5.2), nuk janë regjistruar zhvillime të reja strukturore për krijimin e mekanizmave të rinj, megjithatë shkëmbimi i informacionit vazhdon në mënyrë aktive përmes platformës kombëtare të raportimit të incidenteve dhe kanaleve të NATO-s, përfshirë përdorimin e platformave MISP dhe përfaqësimin në strukturat qendrore të aleancës.

Progres më i dukshëm është shënuar në aspektin operacional dhe teknologjik (Objektivi 5.3). Gjatë vitit 2025 u realizua optimizimi dhe zgjerimi i përdorimit të platformave SIEM/SOAR për monitorim të avancuar dhe detektim të hershëm të kërcënimeve hibride, përmes automatizimit të proceseve dhe integrimit të burimeve të inteligjencës së kërcënimeve. Është vijuar ndërgjegjësimi i vazhdueshëm i përdoruesve dhe administratorëve, si dhe pjesëmarrja në aktivitete të organizuara nga AKSK dhe NATO. Gjithashtu, janë përditësuar të gjitha Procedurat Standarde të Veprimit bazuar në analizën e rreziqeve të fundit. Në fushën e inteligjencës artificiale është realizuar një vlerësim funksional i një platforme AI për analizimin dhe parashikimin e kërcënimeve, duke shërbyer si bazë për integrime të mundshme të ardhshme.

Në tërësi, viti 2025 karakterizohet nga konsolidimi i kapaciteteve ekzistuese, përmirësimi i proceseve operacionale dhe forcimi i bashkëpunimit institucional, ndërsa zhvillimet strukturore dhe strategjike mbeten të kufizuara.

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

Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP)

Gjatë vitit 2025, në kuadër të Objektivit 5.1, është vijuar puna për Masën 5.1.1. Rishikimi i kuadrit ligjor ekzistues për adresimin e mbrojtjes ndaj kërcënimeve hibride, ku AKEP ka kontribuar me opinione për aktet ligjore dhe nënligjore në fushën e komunikimeve elektronike, bazuar në ligjin nr. 54/2024. Njëkohësisht, në zbatim të Masës 5.1.2. Përditësimi i strategjive ekzistuese për përputhje me zhvillimet e reja teknologjike dhe taktikat e kërcënimeve hibride, AKEP është në proces përditësimi të akteve rregullatore, përfshirë këshillimin publik të projektrregullores për masat teknike dhe organizative për sigurinë e rrjeteve dhe shërbimeve të komunikimeve elektronike.

Në drejtim të bashkëpunimit ndërinstitucional, në kuadër të Masës 5.1.3. Krijimi i strukturave përgjegjëse për bashkëpunimin ndërinstitucional për kërcënimet hibride, AKEP merr pjesë në grupe pune që lidhen me sigurinë kibernetike dhe mbrojtjen e fëmijëve *online*. Mekanizmat mbikëqyrës janë forcuar përmes zbatimit të Masës 5.1.4. Implementimi i mekanizmave mbikëqyrës që monitorojnë pajtueshmërinë me kuadrin ligjor, përmes funksionimit të njësisë së inspektimit që monitoron zbatimin e ligjit nr. 54/2024 nga operatorët dhe ISP-të. Po ashtu, në zbatim të Masës 5.1.5. Harmonizimi i legjislacionit kombëtar me atë ndërkombëtar për qasje të përbashkët ndaj kërcënimeve hibride, ligji nr. 54/2024 është përafruar pjesërisht me Direktivën (BE) 2018/1972. Për ngritjen e kapaciteteve institucionale, në kuadër të Masës 5.1.6. Ngritja e kapaciteteve për institucionet përkatëse mbi *acquis* të BE-së, stafi i AKEP ka marrë pjesë në rreth 18 aktivitete trajnuese kombëtare dhe ndërkombëtare.

Në kuadër të Objektivit 5.2, për zbatimin e Masës 5.2.1. Krijimi i një mekanizmi kombëtar për koordinimin e reagimit ndaj kërcënimeve hibride, AKEP ka caktuar përfaqësuesin e tij në ekipin kombëtar të reagimit ndaj emergjencave dhe krizave të sigurisë kibernetike. Gjithashtu, në zbatim të Masës 5.2.2. Zhvillimi i mekanizmave për shkëmbimin e informacionit mes institucioneve kombëtare dhe ndërkombëtare, është forcuar bashkëpunimi me organizma si BEREC dhe ITU për shkëmbim informacioni dhe ekspertize. Në të njëjtën linjë, Masa 5.2.4. Përfshirja e partneriteteve publike dhe private për monitorimin dhe reagimin ndaj kërcënimeve hibride zbatohet përmes bashkëpunimit të vazhdueshëm me operatorët e komunikimeve elektronike për rritjen e sigurisë kibernetike.

Në kuadër të Objektivit 5.3, në zbatim të Masës 5.3.3. Hartimi i fushatave ndërgjegjësuese për rreziqet nga dezinformimi dhe sulmet kibernetike, është planifikuar zhvillimi gjatë vitit 2026 i një fushatë sensibilizuese për tregtinë elektronike dhe sigurinë digjitale.

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

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.

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 mbetet vetëm një dokument formal, por një instrument aktiv që drejton transformimin digjital të sigurt dhe të qëndrueshëm të vendit.

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