VENDIM
Nr. 606, datë 23.10.2025

PËR MIRATIMIN E STRATEGJISË KOMBËTARE PËR SIGURINË KIBERNETIKE 2025–2030 DHE TË PLANIT TË VEPRIMIT 2025–2027

Në mbështetje të nenit 100 të Kushtetutës dhe të pikave 4 e 5, të nenit 6, të ligjit nr. 25/2024, "Për sigurinë kibernetike", me propozimin e Kryeministrit, Këshilli i Ministrave

VENDOSI:

1. Miratimin e Strategjisë Kombëtare për Sigurinë Kibernetike 2025–2030 dhe të planit të saj të veprimit 2025–2027.
2. Vendimi nr. 1084, datë 24.12.2020, i Këshillit të Ministrave, "Për miratimin e Strategjisë Kombëtare për Sigurinë Kibernetike dhe planit të veprimit 2020–2025", shfuqizohet.
3. Ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike, ministritë dhe institucionet e tjera përgjegjëse të përcaktuara në strategji dhe në planin e veprimit për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

ZËVENDËSKRYEMINISTËR
Belinda Balluku

Politika	Objektivi specifik		Rezultate	Institucioni përgjegjës	Institucioni shpenzues	Kostoja totale	PBA			Donatorë			Hendek
							Viti 2025	Viti 2026	Viti 2027	Viti 2025	Viti 2026	Viti 2027	
Politika 1: Mbrojtja e Infrastrukturës Digjitale (Proceset, kapacitetet njerëzore dhe teknologjia)	Objektivi specifik. 0.1 Hartimi dhe zbatimi i kuadrit ligjor për Sigurinë Kibernetike		1.0.1.1 Hartimi i akteve nënligjore në zbatim të ligjit nr. 25/2024, "Për sigurinë kibernetike".	AKSK	AKSK	2,365,164	788,388	788,388	788,388	-			-
			1.0.1.2 Harmonizimi i kuadrit ligjor me acquis e BE-se	AKSK	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.0.1.3 Hartimi i marrëveshjeve kombëtare dhe ndërkombëtare në fushën e sigurisë kibernetike.	AKSK	AKSK	4,680,396	1,560,132	1,560,132	1,560,132	-			-
			1.0.1.4 Mbikëqyrja e zbatimit të ligjit "Për sigurinë kibernetike" nëpërmjet zhvillimit të kontrolleve periodike të OIKI/OIRI.	AKSK	AKSK	2,787,330	929,110	929,110	929,110	-			-
					Subtotal objektivi	14,563,218	4,854,406	4,854,406	4,854,406	-	-	-	-
	1.1. Proceset	1.1.2. Nënobjektivi i Përmirësimi i Kapaciteteve Monitoruese dhe Mbrojtjes se Sisteme ve	1.1.2.1 Përmirësimi dhe standardizimi i procedurave të monitorimit të rrjeteve dhe sistemeve të informacionit, duke përfshirë raportimin dhe reagimin në kohë reale ndaj incidenteve kibernetike.	AKSK/AKSHI	AKSK/AKSHI	12,643,452	4,214,484	4,214,484	4,214,484	-			-
			1.1.2.2 Monitorimi i kërcënimeve kibernetike në hapësirën digjitale të Shqipërisë nëpërmjet inteligjencës kibernetike	AKSK/AKSHI/MM/PSH/SHISH	AKSK	11,533,860	3,844,620	3,844,620	3,844,620	-			-
			1.1.2.3 Përditësimi i masave të sigurisë dhe verifikimit të implementimit të tyre nga OIKI/OIRI, për të reflektuar ndryshimet ne legjislacion, teknologji dhe standarde.	AKSK	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.1.2.4 Hartimi i udhëzimeve dhe protokolleve të sigurisë në OIKI dhe OIRI.	AKSK	AKSK	12,419,568	4,139,856	4,139,856	4,139,856	-			-
			1.1.2.5 Rishikimi periodik i politikave dhe procedurave të sigurisë bazuar në evoluimin e kërcënimeve dhe teknologjisë.	AKSK	AKSK	7,095,492	2,365,164	2,365,164	2,365,164	-			-
			1.1.2.6 Rishikimi i masave të sigurisë kibernetike dhe përfshirja në to e krijimit të ambientit të sigurt në *Cloud* (PaaS, SaaS, IaaS etj.).	AKSK	AKSK	-	-	-	-	-			-
			1.1.2.7. Përmirësimi i procedurave në lidhje me vlerësimin dhe testimin e rrjeteve dhe sistemeve të teknologjisë së informacionit	AKSK	AKSK	-	-	-	-	-			-
			1.1.2.8 Hartimi i procedurave në lidhje me përdorimin e teknologjive IoT, OT, ICS, SCADA dhe teknologjive të avancuara.	AKSK	AKSK	-	-	-	-	-			-
					Subtotal nënobjektivi	48,422,700	16,140,900	16,140,900	16,140,900	-	-	-	-
		Nënobjektivi specifik. 1.1.3 (Proceset) Qeverisja kibernetike dhe Menaxhimi i Rreziqeve	1.1.3.1 Implementimi dhe rishikimi i metodologjisë për vlerësimin e rreziqeve kibernetike të të gjitha sistemeve dhe rrjetave ne OIKI dhe OIRI.	AKSK	AKSK	3,120,264	1,040,088	1,040,088	1,040,088	-			-
			1.1.3.2 Vlerësimi 6-mujor i rreziqeve kibernetike përmes identifikimit të dobësive, kërcënimeve teknologjike dhe gjeopolitike si dhe mundësive për sulme kibernetike.	AKSK	AKSK	6,240,528	2,080,176	2,080,176	2,080,176	-			-
			1.1.3.3 Krijimi i mekanizmave të shkëmbimit të informacionit mbi rreziqet kibernetike me institucionet publike dhe OIRI/OIKI.	AKSK/AKSHI	AKSK	150,000,000	150,000,000	-	-	-			-
			1.1.3.4 Vlerësimi i sigurisë kibernetike në nivel sektorial dhe kombëtar.	AKSK	AKSK	6,290,132	520,044	520,044	5,250,044	-			-
					Subtotal nënobjektivi	165,650,924	153,640,308	3,640,308	8,370,308	-	-	-	-
		Nënobjektivi specifik.1.1.4 (Proceset) Zhvillimi i planeve të reagimit dhe menaxhimit të incidenteve kibernetike	1.1.4.1 Rishikimi dhe përmirësimi i planeve të reagimit dhe menaxhimit të incidenteve kibernetike në nivel kombëtar dhe sektorial.	AKSK	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.1.4.2 Rishikimi i një plani kombëtar të reagimit dhe menaxhimit të incidenteve kibernetike pas çdo incidenti në OIRI/OIKI.	AKSK	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.1.4.3 Rishikimi i procedurës së komunikimit në rast incidenti kibernetik.	AKSK	AKSK	3,570,804	1,190,268	1,190,268	1,190,268	-			-
			1.1.4.4 Përditësimi i procedurës për menaxhimin e krizës kibernetike në nivel kombëtar .	AKSK	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.1.4.5 Implementimi i mekanizmave të avancuar për gjurmimin e sulmeve kibernetike, duke përdorur analiza forensike dhe korelacion të të dhënave të incidenteve.	AKSK/AKSHI/MM	AKSK/AKSHI/MM	305,643,656				61,128,731	122,257,462	122,257,462	
			1.1.4.6 Hartimi i raportit për investigimin e thellë të sulmeve kibernetike në sistemet e ruajtjes së të dhënave.	AKSK/PSH	AKSK	9,460,656	3,153,552	3,153,552	3,153,552	-			-
					Subtotal nënobjektivi	332,866,100	9,074,148	9,074,148	9,074,148	61,128,731	122,257,462	122,257,462	-
		Nënobjektivi specifik. 1.1.5 (Proceset) Garantimi i transaksioneve	1.1.5.1 Harmonizimi i legjislacionit vendës, në fushën e identifikimit elektronik, shërbimeve të besuara, dhe Portofolit të Identitetit Digjital me kuadrin rregullator të Bashkimit Evropian eIDAS 1.0 dhe eIDAS 2.0	AKSK	AKSK	7,095,492	2,365,164	2,365,164	2,365,164	-			-
			1.1.5.2 Hartimi i akteve nënligjore në kuadër të	AKSK	AKSK	9,460,656	3,153,552	3,153,552	3,153,552	-			-

		elektronike përmes Shërbimeve të Besuara	legjislacionit për identifikimin elektronik, shërbimet e besuara, dhe Portofolin e Identitetit Digital.										
			1.1.5.3 Nënshkrimi i marrëveshjeve me vendet e Ballkanit perëndimor për njohjen e shërbimeve të besuara	AKSK	AKSK	7,095,492	2,365,164	2,365,164	2,365,164	-			-
			1.1.5.4 Monitorimi i vepримtarisë së ofruesve të kualifikuar të shërbimeve të besuara, për të garantuar përputhshmërinë me kërkesat ligjore në fuqi.	AKSK	AKSK	3,570,804	1,190,268	1,190,268	1,190,268	-			-
					Subtotal nënobjektivi	27,222,444	9,074,148	9,074,148	9,074,148	-	-	-	-
		Nënobjektivi specifik. 1.1.6 Implementimi i Skemës së Certifikimit të Sigurisë Kibernetike	1.1.6.1 Hartimi i Skemës së Certifikimit të Sigurisë Kibernetike	AKSK	AKSK	-	-	-	-	-			-
			1.1.6.2. Akreditimi i Organeve të Vlerësimit të Konformitetit (OVK)	DPA	DPA	-	-	-	-	-			-
			1.1.6.3. Autorizimi dhe regjistrimi i Organeve të Vlerësimit të Konformitetit (OVK).	AKSK	AKSK	-	-	-	-	-			-
					Subtotal nënobjektivi	-	-	-	-	-	-	-	-
					Subtotal objektivi	574,162,168	187,929,504	37,929,504	42,659,504	61,128,731	122,257,462	122,257,462	-
	1.2. Kapacitetet Njerëzore	Nënobjektivi specifik. 1.2.1 (Kapacitete njerëzore): promovimi dhe zhvillimi i kulturës kibernetike	1.2.1.1. Hartimi dhe zbatimi i fushatave ndërgjegjësuese për higjienën kibernetike dhe praktikat më të mira të sigurisë, me fokus punonjësit e OIKI-së dhe OIRI-t.	AKSK/AKSHI	AKSK	9,460,656	3,153,552	3,153,552	3,153,552	-			-
			1.2.1.2. Zhvillimin e fushatave të ndërgjegjësimit mbi promovimin e përdorimit të shërbimeve të besuara.	AKSK	AKSK	1,190,268	396,756	396,756	396,756	-			-
			1.2.1.3. Zhvillimi i një plani trajnimesh të dedikuara për sigurinë kibernetike.	AKSK	AKSK	396,756	132,252	132,252	132,252	-			-
			1.2.1.4. Trajnime për punonjësit e OIKI-së dhe OIRI-t.	AKSK	AKSK	1,069,108,872	170,000,000	-	-	179,821,774	359,643,549	359,643,549	
					Subtotal nënobjektivi	1,080,156,552	173,682,560	3,682,560	3,682,560	179,821,774	359,643,549	359,643,549	-
		Nënobjektivi specifik. 1.2.2 (Kapacitete njerëzore): rritja e kapaciteteve profesionale	1.2.2.1 Rishikimi dhe integrimi i sigurisë kibernetike në kurrikulat e arsimit parauniversitar.	MA/AKSK	AKSK	6,307,104	2,102,368	2,102,368	2,102,368	-			-
			1.2.2.2 Rritja e aftësive teknike dhe përmirësimi i përvojave praktike të profesionistëve të sigurisë kibernetike përmes pjesëmarrjes aktive në trajnime teknike periodike, aktivitete ndërkombëtare, dhe konkurse teknologjike që përfshijnë zgjidhjen e kërcënimeve dhe rasteve reale.	AKSK/AKSHI	AKSK	5,770,000	5,770,000	-	-	-			-
			1.2.2.3 Identifikimi, rekrutimi dhe zhvillimi i talenteve të reja në sigurinë kibernetike përmes trajnimeve, mentorimit dhe mundësive të karrierës	AKSK/AKSHI	AKSK	12,643,452	4,214,484	4,214,484	4,214,484	-			-
			1.2.2.4 Krijimi i laboratorëve praktikë të sigurisë kibernetike për ushtrime dhe simulime reale.	AKSK	AKSK	360,820,856	37,088,600			64,746,451	129,492,902	129,492,902	
			1.2.2.5 Ngritja e kapaciteteve të stafeve shkollore si dhe organizimi i fushatave sensibilizuese në shkolla "Kundër radikalizimit dhe ekstremizmit të dhunshëm *online*".	CVE /MA/ASHDMF	CVE	185,859	61,953	61,953	61,953	-			-
			1.2.2.6 Zhvillimi dhe shpërndarja e kundër-narrativave për të rritur tolerancën dhe për të luftuar gjuhën e urrejtjes *online* mbi radikalizmin dhe ekstremizmin e dhunshëm.	CVE /MA	CVE	371,721	123,907	123,907	123,907	-			-
					Subtotal nënobjektivi	386,098,992	49,361,312	6,502,712	6,502,712	64,746,451	129,492,902	129,492,902	-
					Subtotal objektivi	1,466,255,544	223,043,872	10,185,272	10,185,272	244,568,226	489,136,451	489,136,451	-
	1.3. Teknologji	Nënobjektivi specifik. 1.3.1 (Teknologji) përdorimi dhe integrimi i teknologjive të avancuara	1.3.1.1 Implementimi dhe integrimi i teknologjive të avancuara si Inteligjenca Artificiale (AI) për zbulimin, parandalimin dhe reagimin ndaj sulmeve kibernetike.	AKSK/AKSHI	AKSK	5,765,009,080	3,331,672,720			-			2,433,336,360
			1.3.1.3 Zhvillimi i politikave të bazuara në *blockchain* për të siguruar integritetin dhe transparencën e transaksioneve digjitale.	AKSK/AKSHI	AKSHI	-	-	-	-	-			-
			1.3.1.4 Përmirësimi i laboratorëve të testimit dhe simulimit të kërcënimeve kibernetike.	AKSK	AKSK	442,269,688	-			88,453,938	176,907,875	176,907,875	
			1.3.1.5 Përdorimi i sistemeve të automatizuara për përditësimin dhe menaxhimin e sigurisë.	AKSK/AKSHI	AKSK	450,000,000	-	-		90,000,000	180,000,000	180,000,000	
					Subtotal nënobjektivi	6,657,278,768	3,331,672,720	-	-	178,453,938	356,907,875	356,907,875	2,433,336,360
		Nënobjektivi specifik. 1.3.2 (Teknologji) - monitorimi, zbulimi dhe mbrojtje kibernetike, duke shfrytëzuar teknologjitë e avancuara.	1.3.2.1. Implementimi i mekanizmave për mbrojtjen proaktive nga kërcënimet e avancuara të vazhdueshme (APT – Advanced Persistent Threats).	AKSK/AKSHI/SHISH/MM	AKSK	895,000,000	-	-	-	179,000,000	358,000,000	358,000,000	
			1.3.2.2. Përdorimi i *cloud computing* për ruajtjen dhe mbrojtjen e të dhënave kritike.	AKSK/AKSHI	AKSK	-	-	-	-	-			-
					Subtotal nënobjektivi	895,000,000	-	-	-	179,000,000	358,000,000	358,000,000	-
		Nënobjektivi specifik. 1.3.3	1.3.3.1. Zhvillimi i politikave për të siguruar integrimin e masave të sigurisë në të gjitha fazat e ciklit të jetës së	AKSK/AKSHI	AKSK	2,660,400	886,800	886,800	886,800	-			-

		(Teknologji) - Implementimi i kornizës *"secure by design"* për infrastrukturat digitale	sistemeve digitale.										
			1.3.3.2 Hartimi i udhëzimeve për infrastrukturat/operatorët mbi parimet e *"secure by design"*.	AKSK/AKSHI	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.3.3.3 Krijimi i protokolleve/manualeve për sigurimin e pajisjeve IoT *(Internet of Things)* dhe mbrojtjen e tyre nga sulmet.	AKSK/AKEP	AKSK/AKEP	1,190,268	396,756	396,756	396,756	-			-
					Subtotal nënobjektivi	8,580,996	2,860,332	2,860,332	2,860,332	-	-	-	-
		Nënobjektivi specifik. 1.3.4 (Teknologji) Menaxhimi efektiv i teknologjive të vjetruara	1.3.4.1 Hartimi i një plani kombëtar për identifikimin dhe përditësimin/izolimin e teknologjive të vjetruara në sistemet kritike.	AKSK	AKSK	1,560,132	520,044	520,044	520,044	-			-
			1.3.4.2 Zhvillimi i një programi për migrimin drejt teknologjive më të sigurta dhe të qëndrueshme.	AKSK/AKSHI	AKSK/AKSHI	2,365,164	788,388	788,388	788,388	-			-
			1.3.4. 3 Realizimi i kontrolleve periodike ndaj teknologjive të vjetruara.	AKSK	AKSK	6,307,104	2,102,368	2,102,368	2,102,368	-			-
					Subtotal nënobjektivi	10,232,400	3,410,800	3,410,800	3,410,800	-	-	-	-
		Nënobjektivi specifik. 1.3.5 (Teknologji) përdorimi i teknologjive alternative kompensuese për sigurinë kibernetike	1.3.5.1 Promovimi dhe përdorimi i teknologjive alternative kompensuese për të mbështetur sigurinë kibernetike dhe për të ofruar zgjidhje në raste të kufizimeve teknologjike ose financiare.	AKSK	AKSK	1,560,132	520,044	520,044	520,044	-			-
			1.3.5.2 Përdorimi i platformave alternative kur teknologjitë me pagesë nuk janë të disponueshme.	AKSK	AKSK	4,160,352	1,386,784	1,386,784	1,386,784	-			-
					Subtotal nënobjektivi	5,720,484	1,906,828	1,906,828	1,906,828	-	-	-	-
					Subtotal objektivi	7,576,812,648	3,339,850,680	8,177,960	8,177,960	357,453,938	714,907,875	714,907,875	2,433,336,360
					Subtotal i politikës 1	9,631,793,578	3,755,678,462	61,147,142	65,877,142	663,150,894	1,326,301,789	1,326,301,789	2,433,336,360
Politika 2: Mbrojtja *Online* e Qytetarëve dhe Nxitja e Kulturës Kibernetike	Objektivi 2.1: Hartimi dhe zhvillimi i Planit Kombëtar për Ndërgjegjësimin e Qytetarëve (PKNQ)		2.1.1 Analizimi i situatës aktuale lidhur me fushatat/programet e ndërgjegjësimit dhe vlerësimi i nevojave për rishikimin e tyre.	AKSK/MSHMS	AKSK	2,055,000	685,000	685,000	685,000	-			-
			2.1.2 Zhvillimi i një programi që përfshin trajnime të vazhdueshme të segmentuara/fragmentizuara në varësi të grupeve të interesit dhe nevojave specifike që ata kanë, mbi kërcënimet kibernetike dhe mënyrat për t'i parandaluar ato, si *phishing* dhe keqpërdorimi i të dhënave.	AKSK	AKSK	793,512	264,504	264,504	264,504	-			-
			2.1.3 Përgatitja dhe shpërndarja e materialeve edukative të qarta dhe të aksesueshme për qytetarët, si dhe në një gjuhë të kuptueshme dhe miqësore për fëmijët mbi higjienën kibernetike dhe sigurinë në internet.	AKSK/MSHMS	AKSK	6,667,275	2,222,425	2,222,425	2,222,425	-			-
			2.1.4 Krijimi i fushatave publicitare për të promovuar ndërgjegjësimin dhe mitjen e njohurive mbi sigurinë kibernetike nëpërmjet kanaleve të ndryshme mediatike.	AKSK	AKSK	30,000,000	10,000,000	10,000,000	10,000,000	-			-
			2.1.5 Promovimi për mitjen e përdorimit të "RED BUTTON" për raportimin e përmbajtjeve të paligjshme.	CVE /AKSK	AKSK	-	-	-	-	-			-
					Subtotal objektivi	39,515,787	13,171,929	13,171,929	13,171,929	-	-	-	-
	Objektivi specifik 2.2: Hartimi i një kornize ligjore për qasjen gjithëpërfshirëse të qytetarëve		2.2.1 Identifikimi i nevojës për ndryshime në legjislacionin ekzistues për të forcuar mbrojtjen *online* të qytetarëve.	AKSK	AKSK	1,560,132	520,044	520,044	520,044	-			-
			2.2.2 Përgatitja e një projektligji për mbrojtjen *online* të qytetarëve nga kërcënimet e mundshme kibernetike.	AKSK	AKSK	4,160,352	1,386,784	1,386,784	1,386,784	-			-
					Subtotal objektivi	5,720,484	1,906,828	1,906,828	1,906,828	-	-	-	-
	Objektivi specifik 2.3: Krijimi i mekanizmave të nevojshëm për mbrojtjen *online* të fëmijëve.		2.3.1 Rishikimi i kurrikulës së arsimit parauniversitar për të evidentuar përfshirjen e sigurisë kibernetike dhe rekomandimi i përmirësimeve të nevojshme.	AKSK/MA	MA	3,153,552	-	3,153,552	-	-			-
			2.3.2 Trajnimi i stafit mësimor mbi sigurinë kibernetike dhe hartimi i një programi të rregullt për ngritjen e kapaciteteve në shkolla.	AKSK/MA	MA	-	-	-	-	-			-
			2.3.3 Integrimi i moduleve për sigurinë kibernetike dhe mbrojtjen *online* të fëmijëve dhe të rinjve në kurrikulat mësimore në të gjitha nivelet.	AKSK/MA	MA	-	-	-	-	-			-
			2.3.4 Realizimi i fushatave për informimin dhe edukimin e prindërve mbi përdorimin e aplikacioneve dhe platformave të sigurisë kibernetike që mundësojnë kontrollin prindëror.	AKSK/MA	AKSK	3,221,532	1,073,844	1,073,844	1,073,844	-			-
					Subtotal objektivi	6,375,084	1,073,844	4,227,396	1,073,844	-	-	-	-
	Objektivi specifik 2.4: Nxitja e barazisë gjinore në hapësirën digitale		2.4.1 Promovimi i edukimit dhe karrierës së grave dhe vajzave nga të gjitha grupet në fushën e teknologjisë dhe sigurisë kibernetike.	AKSK/AKSHI/MSHMS	AKSK	30,211,293	10,070,431	10,070,431	10,070,431	-			-
			2.4.2 Organizimi i trajnimeve vjetore të dedikuara për vajzat dhe gratë në këtë fushë.	AKSK	AKSK	2,147,688	715,896	715,896	715,896	-			-
			2.4.3 Zhvillimi i fushatave për promovimin e mundësive të barabarta për gratë në sektorin digital.	AKSK	AKSK	2,326,662	775,554	775,554	775,554	-			-
					Subtotal objektivi	34,685,643	11,561,881	11,561,881	11,561,881	-	-	-	-

	Objektivi specifik 2.5: Krijimi i mekanizmave të duhur për mbrojtjen e SME-ve *online*	2.5.1 Promovimi i edukimit te SME-të në fushën e teknologjisë dhe sigurisë kibernetike.	AKSK	AKSK	5,470,056	1,823,352	1,823,352	1,823,352	-			-
		2.5.2 Përgatitja e udhëzimeve mbi masat e sigurisë kibernetike te SME-të.	AKSK	AKSK	5,470,056	1,823,352	1,823,352	1,823,352	-			-
		2.5.3 Organizimi i trajnimeve vjetore të dedikuara për Punonjësit e SME-ve.	AKSK	AKSK	5,470,056	1,823,352	1,823,352	1,823,352	-			-
				Subtotal objektivi	16,410,168	5,470,056	5,470,056	5,470,056	-	-	-	-
	Objektivi specifik 2.6: Krijimi i mekanizmave të nevojshëm për mbrojtjen dhe fuqizimin e grupeve të nënpërfaqësuara	2.6.1 Krijimi i një platforme kombëtare me mjete edukative dhe interaktive për rritjen e ndërgjegjësimit mbi sigurinë *online*.	AKSK	AKSK	136,000,000	136,000,000			-			-
		2.6.2 Hartimi dhe shpërndarja e materialeve edukative të përshtatura për grupet e nënpërfaqësuara.	AKSK	AKSK	3,997,000	1,332,333	1,332,333	1,332,333	-			-
				Subtotal objektivi	139,997,000	137,332,333	1,332,333	1,332,333	-	-	-	-
				Subtotal i politikës 2	242,704,166	170,516,871	37,670,423	34,516,871	-	-	-	-
Politika 3: Forcimi i Bashkëpunimit Ndërkombëtar	Objektivi specifik 3.1: Harmonizimi i politikave dhe legjislacionit	3.1.1 Ngritja e një grupi pune për të analizuar dhe rekomanduar ndryshime legjislative që do të harmonizohen me direktivat dhe standardet ndërkombëtare.	AKSK	AKSK	-	-	-	-	-			-
		3.1.2 Realizimi i fushatave ndërgjegjësuese për autoritetet publike dhe sektorin privat mbi implementimin e politikave dhe legjislacionit të sigurisë kibernetike.	AKSK	AKSK	-	-	-	-	-			-
				Subtotal objektivi	-	-	-	-	-	-	-	-
	Objektivi specifik 3.2: Forcimi i bashkëpunimit rajonal (WB6) dhe ndërkombëtar	3.2.1 Hartimi i një programi rajonal për trajnim dhe simulime të përbashkëta mbi sulmet kibernetike për institucionet publike dhe sektorin privat.	AKSK/MEPJ	AKSK	29,775,000	9,925,000	9,925,000	9,925,000	-			-
		3.2.2 Organizimi i tryezave rajonale për ndarjen e praktikave më të mira.	AKSK/MEPJ	AKSK	-	-	-	-	-			-
				Subtotal objektivi	29,775,000	9,925,000	9,925,000	9,925,000	-	-	-	-
	Objektivi specifik 3.3: Zhvillimi i diplomacisë kibernetike	3.3.1 Përgatitja e një plani kombëtar që përcakton qartë objektivat dhe partnerët strategjikë për bashkëpunim në sigurinë kibernetike.	AKSK/MEPJ	AKSK	1,330,200	443,400	443,400	443,400	-			-
		3.3.2 Përfshirja në mekanizmat ndërkombëtarë për bashkëpunim në fushën e sigurisë kibernetike, me fokus ndarjen e përvojave praktike dhe forcimin e dialogut ndërinstitucional mbi sfidat dhe zgjidhjet strategjike.	AKSK	AKSK/MEPJ	-	-	-	-	-			-
		3.3.3 Ngritja e kapaciteteve kombëtare për diplomacinë kibernetike.	AKSK/AKSHI/MEPJ	AKSK/AKSHI/MEPJ	-	-	-	-	-			-
				Subtotal objektivi	1,330,200	443,400	443,400	443,400	-	-	-	-
				Subtotal i politikës 3	31,105,200	10,368,400	10,368,400	10,368,400	-	-	-	-
Politika 4 - Nxitja e Inovacionit dhe Kërkimit Shkencor në Sigurinë Kibernetike	Objektivi 4.1 Ngritja e Qendrës Kombëtare të Ekselencës për Sigurinë Kibernetike	4.1.1 Hartimi dhe miratimi i rregulloreve dhe udhëzimeve për ngritjen dhe funksionimin e QKESK-së.	AKSK/MA /MEI	AKSK	-	-	-	-	-			-
		4.1.2 Krijimi i mekanizmave për monitorimin dhe vlerësimin e performancës së QKESK-së.	AKSK/MA /MEI	AKSK	-	-	-	-	-			-
		4.1.3 Pajisja e QKESK-së me laboratorë kërkimorë dhe infrastrukturë për testimin e teknologjive të reja.	AKSK/MEI	AKSK	-	-	-	-	-			-
		4.1.4 Nxitja e bashkëpunimit Publik-Privat për zhvillimin e projekteve kërkimore dhe inovative ndërmjet institucioneve publike, akademisë dhe sektorit privat.	AKSHI/AKSK/MEI	MEI	-	-	-	-	-			-
		4.1.5 Nxitja dhe promovimi i shkëmbimit të njohurive, eksperiencave mbi zgjidhjet inovative në fushën e sigurisë kibernetike.	MEI/AKSK/AKSHI	MEI	-	-	-	-	-			-
				Subtotal objektivi	-	-	-	-	-	-	-	-
	Objektivi 4.2. Mbështetja e *startup*-eve në fushën e sigurisë kibernetike	4.2.1 Krijimi i mekanizmave për nxitjen dhe lehtësimin e funksionimit të *startup*-eve të ne fushën e teknologjisë se informacionit dhe sigurisë kibernetike.	MEI/AKSK	MEI	-	-	-	-	-			-
		4.2.2 Sigurimi i hapësirave mbështetëse për *startup*-e *(tech hubs*, inkubatorë).	MEI/AKSK	MEI	-	-	-	-	-			-
		4.2.3 Ofrimi i laboratorit aktual për zhvillimin dhe testimin e zgjidhjeve inovative si dhe permiresimin e tij.	AKSK	AKSK	-	-	-	-	-			-
		4.2.4 Përfshirja e *startup*-eve në projektet kërkimore për testimin e teknologjive të reja.	MEI/AKSK	MEI	-	-	-	-	-			-
		4.2.5 Nxitja e partneriteteve strategjike me kompani të mëdha për të mundësuar integrimin e *startup*-eve inovative në ekosistemin kombëtar të sigurisë kibernetike.	MEI/AKSK	MEI	-	-	-	-	-			-
		4.2.6 Mbështetja e projekteve kërkimore ndërmjet *startup*-eve dhe institucioneve të arsimit të lartë.	AKSK/MA/MEI/	MEI	-	-	-	-	-			-
		4.2.7 Organizimi i *hackathon*-eve dhe konkurseve për zgjidhje inovative në sigurinë kibernetike.	MEI/AKSK	AKSK	90,000,000	30,000,000	30,000,000	30,000,000	-			-
				Subtotal objektivi	90,000,000	30,000,000	30,000,000	30,000,000	-	-	-	-
	Objektivi 4.3. Zhvillimi	4.3.1 Zhvillimi i programeve kombëtare të financimit	MEI/AKSK	MEI	-	-	-	-	-			-

	i programeve të financimit për kërkim dhe inovacion në sigurinë kibernetike.	me zhvillimin e kërkimit dhe inovacionit në sigurinë kibernetike.										
		4.3.2 Krijimi i një fondi kombëtar për mbështetjen e kërkimeve në sigurinë kibernetike	MEI/MA/AKSK	AKSK	-	-	-	-	-			-
		4.3.3 Lehtësimi i aksesit në grantet e BE-së dhe donatorët ndërkombëtarë për kërkim dhe zhvillim	MEI/AKSK	MEI/AKSK	-	-	-	-	-			-
		4.3.4 Ofrimi i stimujve fiskalë për bizneset që investojnë në teknologji të sigurta dhe kërkim shkencor	MEI/AKSK	MEI	-	-	-	-	-			-
				Subtotal objektivi	-	-	-	-	-	-	-	-
				Subtotal i politikës 4	90,000,000	30,000,000	30,000,000	30,000,000	-	-	-	-
Politika 5- Mbrojtja ndaj kërcënimeve hibride	Objektivi specifik 5.1 Hartimi i kuadrit ligjor për mbrojtjen ndaj kërcënimeve kibernetike hibride	5.1.1 Rishikimi i kuadrit ligjor ekzistues për adresimin e mbrojtjes ndaj kërcënimeve hibride.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP/MPB	AKSK	3,153,552	-	3,153,552	-	-			-
		5.1.2 Përditësimi i strategjive ekzistuese për përputhjen me zhvillimet e reja teknologjike dhe taktikat e kërcënimeve hibride.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	3,990,600	1,330,200	1,330,200	1,330,200	-			-
		5.1.3 Krijimi i strukturave përgjegjëse për bashkëpunimin ndërinstitucional për kërcënimet hibride.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
		5.1.4 Implementimi i mekanizmave mbikëqyrës që monitorojnë pajtueshmërinë me kuadrin ligjor.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP/MPB	AKSK	4,160,352	1,386,784	1,386,784	1,386,784	-			-
		5.1.5 Harmonizimi i legjislacionit kombëtar me atë ndërkombëtar për të siguruar një qasje të përbashkët në luftën ndaj kërcënimeve hibride.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	MEPJ	-	-	-	-	-			-
		5.1.6 Ngritja e kapaciteteve për institucionet përkatëse mbi acquis të BE-së.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	1,995,300	665,100	665,100	665,100	-			-
				Subtotal objektivi	18,030,132	4,958,860	8,112,412	4,958,860	-	-	-	-
	Objektivi specifik 5.2 Koordinimi ndërinstitucional dhe ndërkombëtar	5.2.1 Krijimi i një mekanizmi kombëtar për koordinimin e reagimit ndaj kërcënimeve hibride.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	8,205,084	2,735,028	2,735,028	2,735,028	-			-
		5.2.2 Zhvillimi i mekanizmave për shkëmbimin e informacionit mes institucioneve kombëtare dhe ndërkombëtare.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	-	-	-	-	-			-
		5.2.3 Organizimi i trajnimeve dhe ushtrimeve të përbashkëta me OIKI/OIRI për përballimin e sulmeve hibride.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	60,000,000	20,000,000	20,000,000	20,000,000	-			-
		5.2.4 Përfshirja e partneriteteve publike dhe private për monitorimin dhe reagimin ndaj kërcënimeve hibride.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	-	-	-	-	-			-
		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.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	-	-	-	-	-			-
		5.2.6 Nxitja e marrëveshjeve te bashkëpunimit ndërkombëtar për mbrojtjen ndaj kërcënimeve hibride.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	-	-	-	-	-			-
				Subtotal objektivi	68,205,084	22,735,028	22,735,028	22,735,028	-	-	-	-
	Objektivi specifik 5.3 Krijimi i mekanizmave të mbrojtjes ndaj kërcënimeve hibride	5.3.1 Implementimi i mjeteve dhe teknologjive te avancuara për monitorim dhe identifikim të hershëm të kërcënimeve hibride.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	-	-	-	-	-			-
		5.3.2 Implementimi i platformave për shkëmbimin e informacionit mbi kërcënimet hibride.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	200,000,000	-	200,000,000	-	-			-
		5.3.3 Hartimi i fushatave ndërgjegjësuese për rreziqet nga dezinformimi dhe sulmet kibernetike.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	3,941,940	1,313,980	1,313,980	1,313,980	-			-
		5.3.4 Përditësimi periodik i protokolleve të emergjencës bazuar në analizën e rreziqeve më të fundit.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	3,153,552	1,051,184	1,051,184	1,051,184	-			-
		5.3.5 Përdorimi i teknologjive të inteligjencës artificiale për analizimin e të dhënave dhe parashikimin e kërcënimeve hibride.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK/AKSHI	-	-	-	-	-			-
				Subtotal objektivi	207,095,492	2,365,164	202,365,164	2,365,164	-	-	-	-
	Objektivi specifik 5. 4 Krijimi i mekanizmave për parandalimin dhe hetimin e krimit kibernetik	5.4.1 Forcimi i bashkëpunimit ndërinstitucional në luftën kundër krimit kibernetik.	MEPJ/AKSK/PSH	PSH	-	-	-	-	-			-
		5.4.2 Përmirësimi i kuadrit ligjor për t'u harmonizuar me legjislacionin dhe konventat ndërkombëtare në fushën e krimeve kibernetike.	MEPJ/PSH	PSH	2,062,500	687,500	687,500	687,500	-			-
				Subtotal objektivi	2,062,500	687,500	687,500	687,500	-	-	-	-
				Subtotal i politikës 5	295,393,208	30,746,552	233,900,104	30,746,552	-	-	-	-
				Grand total	**10,290,996,152**	**3,997,310,285**	**373,086,069**	**171,508,965**	**663,150,894**	**1,326,301,789**	**1,326,301,789**	**2,433,336,360**

	Kostoja totale	Viti 2025	Viti 2026	Viti 2027	Donatorë 2025	Donatorë 2026	Donatorë 2027	Hendek
AKSHI	-	-	-	-	-			-
AKSK	10,284,032,252	3,996,040,169	368,662,401	170,238,849	663,150,894	1,326,301,789	1,326,301,789	2,433,336,360
CVE	557,580	185,860	185,860	185,860	-			-

MAS	-	-	-	-	-			-
MEKI	-	-	-	-	-			-
MEPJ	-	-	-	-	-			-
PSH	2,062,500	687,500	687,500	687,500	-			-
	10,286,652,332	**3,996,913,529**	**369,535,761**	**171,112,209**	**663,150,894**	**1,326,301,789**	**1,326,301,789**	**2,433,336,360**

	Kostoja totale	**Viti 2025**	**Viti 2026**	**Viti 2027**	**Donatorë 2025**	**Donatorë 2026**	**Donatorë 2027**	**Hendek**
AKSHI	-	-	-	-	-	-	-	-
AKSK	10,285,222,520	3,996,436,925	369,059,157	170,635,605	663,150,894	1,326,301,789	1,326,301,789	2,433,336,360
AKEP	-	-	-	-	-	-	-	-
MPB	-	-	-	-	-	-	-	-
MM	-	-	-	-	-	-	-	-
CVE	557,580	185,860	185,860	185,860	-	-	-	-
MA	3,153,552	-	3,153,552	-	-	-	-	-
MEI	-	-	-	-	-	-	-	-
MEPJ	-	-	-	-	-	-	-	-
PSH	2,062,500	687,500	687,500	687,500	-	-	-	-
	10,290,996,152	**3,997,310,285**	**373,086,069**	**171,508,965**	**663,150,894**	**1,326,301,789**	**1,326,301,789**	**2,433,336,360**

STRATEGJIA KOMBËTARE
PËR SIGURINË KIBERNETIKE 2025–2030

Përmbajtja

Qëllimi i politikës 5: Mbrojtja ndaj kërcënimeve hibride

Objektivi specifik 1: Hartimi i kuadrit ligjor për mbrojtjen ndaj kërcënimeve kibernetike hibride

Objektivi specifik 2: Koordinimi ndërinstitucional dhe ndërkombëtar për mbrojtjen ndaj kërcënimeve hibride

Objektivi specifik 3: Krijimi i mekanizmave të mbrojtjes ndaj kërcënimeve hibride

Objektivi specifik 4: Krijimi i mekanizmave për parandalimin dhe hetimin e krimit kibernetik

Zbatimi, përgjegjësia e institucioneve, llogaridhënia

Plani i veprimit dhe burimet financiare për zbatim

PJESA I
KONTEKSTI STRATEGJIK

1. Hyrje

Në një periudhë, ku transformimi digjital po ndikon thellësisht në të gjitha aspektet e jetës shoqërore, ekonomike dhe institucionale, siguria kibernetike ka marrë një rëndësi të jashtëzakonshme kudo në botë. Shqipëria, si pjesë e pandashme e ekosistemit global të informacionit, është e angazhuar të përballet me sfidat dhe të përqafojë mundësitë që ofron hapësira kibernetike, për të siguruar një mjedis digjital të sigurt e të besueshëm për qytetarët, bizneset dhe institucionet e saj.

Strategjia Kombëtare për Sigurinë Kibernetike 2025–2030 është një dokument i rëndësishëm, që pasqyron këtë angazhim dhe përcakton drejtimet strategjike për zhvillimin e forcimin e sigurisë kibernetike në Shqipëri.

Kjo strategji ka si qëllim kryesor forcimin e kapaciteteve kombëtare për të identifikuar, parandaluar e menaxhuar kërcënimet kibernetike, duke përfshirë mbrojtjen e infrastrukturave kritike dhe të rëndësishme të informacionit, mbrojtjen e të dhënave sensitive dhe garantimin e vazhdimësisë së shërbimeve digjitale. Ajo, gjithashtu, synon rritjen e kapaciteteve teknike dhe profesionale të nevojshme për t'u përballur me sfidat e vazhdueshme për mbrojtjen e hapësirës digjitale dhe promovimin e bashkëpunimit ndërkombëtar për të përmirësuar efikasitetin dhe reagimin ndaj incidenteve kibernetike.

Strategjia vendos një kornizë për të rritur gatishmërinë dhe qëndrueshmërinë e sistemeve dhe shërbimeve të informacionit në vend, duke siguruar që Shqipëria të përmbushë standardet e praktikat më të mira ndërkombëtare në këtë fushë. Ajo reflekton harmonizimin e politikave të sigurisë kibernetike me ato të Bashkimit Evropian dhe partnerëve ndërkombëtarë, për të mbështetur zhvillimin e qëndrueshëm të infrastrukturave të informacionit dhe ekonomisë digjitale të vendit.

Një aspekt i rëndësishëm i kësaj strategjie është angazhimi i të gjithë aktorëve, si: institucionet shtetërore, sektori privat, shoqëria civile dhe institucionet e arsimit të lartë, për të krijuar një ekosistem të koordinuar dhe gjithëpërfshirës të sigurisë kibernetike. Kjo do të mundësojë ndarjen e informacionit dhe të burimeve, zhvillimin e politikave të përbashkëta dhe rritjen e ndërgjegjësimit rreth rreziqeve dhe masave të sigurisë.

2. Vlerësimi i situatës aktuale në Shqipëri

Në një kohë kur Shqipëria po implementon çdo ditë e më shumë teknologjitë e informacionit e të komunikimit në çdo fushë të jetës, edhe rreziqet e sigurisë kibernetike po evoluojnë me shpejtësi. Tendencat globale tregojnë një rritje të sulmeve kibernetike, të nxitura nga subjekte të sponsorizuara nga shtete, organizata kriminale dhe grupe keqbërëse. Shteti, ekonomia dhe qeveria shqiptare përballen me kërcënime të vazhdueshme kibernetike, që kërkojnë vëmendje të menjëhershme për të mbrojtur infrastrukturën kritike dhe të rëndësishme të informacionit, rrjetet e sektorit publik dhe të dhënat e qytetarëve.

Në Shqipëri janë bërë hapa të rëndësishëm për forcimin e sigurisë kibernetike. Hartimi i Strategjisë Kombëtare për Sigurinë Kibernetike vendosi një kornizë të qartë për mbrojtjen e

infrastrukturave kritike e të rëndësishme të informacionit dhe menaxhimin e rreziqeve kibernetike. Autoriteti Kombëtar për Sigurinë Kibernetike fuqizoi dhe përmirësoi ndjeshëm proceset e monitorimit, vlerësimit të rreziqeve dhe menaxhimit të kërcënimeve. Disa nga arritjet më të rëndësishme në nivel kombëtar janë rritja e nivelit të zbatimit të masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit, si dhe rritja e kapaciteteve teknike të ekspertëve nëpërmjet trajnimeve dhe kontrolleve rigoroze.

Shqipëria ka intensifikuar ndjeshëm bashkëpunimin me organizata ndërkombëtare, si NATO-ja dhe Bashkimi Evropian, duke siguruar përputhshmëri me normat ndërkombëtare. Përveç kësaj, janë ndërmarrë hapa për rritjen e ndërgjegjësimit dhe edukimit të qytetarëve e bizneseve për sigurinë kibernetike. Shqipëria ka harmonizuar legjislacionin e saj me direktivat e Bashkimit Evropian, duke forcuar kështu mbrojtjen kibernetike në nivel kombëtar e ndërkombëtar.

Sulmet kibernetike të viteve të fundit kanë theksuar rëndësinë e përmirësimit të proceseve të standardizuara për reagimin ndaj incidenteve, përforcimin e kapaciteteve për monitorimin e rrjetit dhe zhvillimin e mekanizmave të qendërzuar për ndarjen efektive të informacionit mbi kërcënimet.

Për më tepër, në Indeksin Global të Sigurisë Kibernetike 2024, Shqipëria ka shënuar një progres të jashtëzakonshëm, duke u ngjitur me 23 vende në renditjen globale, nga vendi i 80-të në vendin e 57-të, dhe duke avancuar nga vendi i 40-të në atë 30-të në Evropë, ku renditet në grupin *"Tier 2",* që përfshin vendet me avancim të shpejtë në sigurinë digjitale.

Në këtë drejtim, Shqipëria është e angazhuar të ndërtojë një hapësirë digjitale të sigurt e të besueshme për qytetarët dhe bizneset, duke fuqizuar qëndrueshmërinë kibernetike të vendit, duke përshpejtuar procesin e integrimit në Bashkimin Evropian dhe duke u pozicionuar si një aktor i fuqishëm dhe i besueshëm në epokën digjitale globale.

Pavarësisht progresit të konsiderueshëm që Shqipëria ka arritur në fushën e sigurisë kibernetike, ende mbeten shumë detyra për t'u realizuar. Sfidat e sigurisë kibernetike bëhen edhe më të mëdha si pasojë e rritjes së vazhdueshme të numrit të sulmeve kibernetike, si dhe nga niveli i lartë dhe sofistikuar i këtyre sulmeve, të cilat shfrytëzojnë teknologjitë më të avancuara. Objektivat e këtyre sulmeve po bëhen gjithnjë e më të gjerë, duke përfshirë jo vetëm sektorin publik, por edhe shërbimet jetike, si shëndetësia, financat, transporti dhe energjia.

Përdorimi i internetit për përhapjen e ideologjive ekstremiste dhe rekrutimin e individëve për qëllime terroriste është një kërcënim në rritje, duke bërë që parandalimi i këtyre aktiviteteve të jetë gjithnjë e më i komplikuar. Në këtë kontekst, siguria kombëtare e Shqipërisë është e lidhur ngushtë me aftësinë për të identifikuar, parandaluar e reaguar ndaj kërcënimeve kibernetike, duke përfshirë ato hibride. Një aspekt kyç i kësaj strategjie është zhvillimi i strukturave të inteligjencës, që janë të specializuara për të monitoruar e parandaluar aktivitete ekstremiste dhe terroriste në hapësirën kibernetike. Në kuadër të luftës kundër terrorizmit, një fokus i rëndësishëm është parandalimi i propagandës ekstremiste dhe rekrutimit *online*. Kjo përfshin përdorimin e teknologjive të avancuara për të identifikuar e mbyllur faqe dhe përmbajtje, që promovojnë dhunën dhe radikalizmin, si dhe krijimin e mekanizmave të bashkëpunimit me aktorët ndërkombëtarë dhe platformat *online*.

Gjithashtu, faktorët socialë po ndikojnë gjithnjë e më shumë, përfshirë bullizmin *online*, shfrytëzimin e fëmijëve dhe të grupeve vulnerabël të shoqërisë, si dhe sulmet ndaj organizatave e individëve, me qëllim dezinformimin dhe përfitimet financiare përmes shkatërrimit të reputacionit, si në nivelin personal, ashtu edhe në atë profesional.

3. Vizioni dhe misioni

3.1 Vizioni

Strategjia Kombëtare për Sigurinë Kibernetike 2025–2030 ka si vizion garantimin e një ekosistemi digjital të sigurt, të qëndrueshëm dhe gjithëpërfshirës, që nxit besimin, inovacionin dhe përparimin ekonomik të vendit.

Duke përqafuar transformimin digjital përmes aplikimit të teknologjive të avancuara si inteligjenca artificiale, superkompjuterat, *blockchain*, strategjia synon forcimin e pozicionit të

Shqipërisë si lider në sigurinë kibernetike në rajon dhe integrimin me politikat e në kornizën ligjore e rregullatore të Bashkimit Evropian.

Përtej mbrojtjes teknike, ky vizion reflekton një angazhim më të gjerë për të mbështetur zhvillimin politik, social dhe ekonomik të vendit, që promovon bashkëpunimin ndërmjet institucioneve, sektorit privat dhe partnerëve ndërkombëtarë, duke krijuar një qasje të unifikuar për adresimin e kërcënimeve dhe të mundësive të reja në epokën digjitale.

Nëpërmjet kësaj strategjie, Shqipëria synon jo vetëm të mbrojë hapësirën e saj digjitale, por edhe të krijojë një kulturë të përgjegjësisë e të ndërgjegjësimit për sigurinë kibernetike. Ky angazhim gjithëpërfshirës do të përmirësojë qëndrueshmërinë e vendit ndaj sfidave të vazhdueshme, duke e bërë Shqipërinë një model për qasje të avancuara në sigurinë kibernetike në rajon dhe më gjerë.

3.2 Misioni

Misioni i Strategjisë Kombëtare të Sigurisë Kibernetike 2025–2030 është krijimi i një mburoje të fortë dhe gjithëpërfshirëse për të mbrojtur qytetarët, institucionet, infrastrukturat kritike e të rëndësishme të informacionit në Republikën e Shqipërisë nga kërcënimet e vazhdueshme dhe në zhvillim të hapësirës kibernetike. Kjo strategji synon të konsolidojë një kuadër të avancuar ligjor, teknik dhe organizativ, të përputhur me standardet evropiane dhe ndërkombëtare, për të garantuar siguri të qëndrueshme dhe zhvillim të ekosistemit digjital kombëtar.

Duke ndërtuar një mjedis të sigurt digjital, kjo strategji synon të fuqizojë qytetarët dhe të krijojë kushte për një shoqëri, ku teknologjia shërben si katalizator i inovacionit dhe progresit. Përmes mbështetjes së një zhvillimi të qëndrueshëm ekonomik dhe shoqëror, strategjia jo vetëm që mbron interesat kombëtarë, por gjithashtu promovon konkurrencën dhe aftësinë e Shqipërisë për të luajtur një rol të rëndësishëm në transformimin digjital të rajonit dhe më gjerë. Misioni thekson, gjithashtu, rëndësinë e bashkëpunimit ndërinstitucional dhe ndërkombëtar për adresimin e sfidave komplekse të sigurisë kibernetike. Ai bazohet në një angazhim për krijimin e një kulture të përgjegjshmërisë kibernetike, duke përfshirë rritjen e ndërgjegjësimit publik dhe ndërtimin e kapaciteteve teknike dhe burimeve njerëzore. Nëpërmjet kësaj strategjie, Shqipëria synon jo vetëm të përballojë kërcënimet kibernetike të së tashmes, por edhe të ndërtojë një themel të fortë për mbrojtjen dhe zhvillimin e sigurt të hapësirës digjitale të së ardhmes, duke rritur qëndrueshmërinë kibernetike në nivel kombëtar.

PJESA II
QËLLIMI I POLITIKAVE DHE OBJEKTIVAT SPECIFIKË TË STRATEGJISË

Objektivat e Strategjisë Kombëtare të Sigurisë Kibernetike 2025–2030 fokusohen në forcimin e mbrojtjes së infrastrukturave kritike dhe të rëndësishme të informacionit në vend, duke krijuar një kuadër ligjor dhe teknik, që siguron vazhdimësinë e shërbimeve dhe stabilitetin e sistemeve të informacionit.

Strategjia synon përmirësimin e bashkëpunimit ndërmjet sektorit publik, privat dhe aktorëve të tjerë për të rritur kapacitetet mbrojtëse dhe për të mundësuar shkëmbimin e informacionit të rëndësishëm në menaxhimin e incidenteve kibernetike.

Një tjetër objektiv kyç është zhvillimi i kapaciteteve teknike dhe profesionale për të përballuar kërcënimet kibernetike, duke investuar në zhvillimin e aftësive dhe në teknologji të avancuara.

Për më tepër, strategjia promovon inovacionin dhe kërkimin shkencor për të përmirësuar aftësitë, me qëllim parashikimin, menaxhimin dhe reagimin ndaj sulmeve kibernetike, si dhe rritjen e ndërgjegjësimit dhe edukimit të shoqërisë mbi sigurinë kibernetike.

Në këtë kuadër, strategjia ka për qëllim përputhshmërinë me normat dhe direktivat e Bashkimit Evropian dhe forcimin e bashkëpunimit me partnerët ndërkombëtarë për të adresuar kërcënimet e sofistikuara dhe ato hibride, që mund të cenojnë sigurinë kombëtare dhe stabilitetin digjital të vendit.

Politikat

Strategjia Kombëtare për Sigurinë Kibernetike të Shqipërisë 2025–2030 është ndërtuar mbi pesë politika kryesore, ku ***mbrojtja e infrastrukturës digjitale*** përbën politikën kryesore të të gjithë strategjisë. Zhvillimet e sigurisë kibernetike, të cilat janë të lidhura ngushtësisht me përparimet teknologjike, ekonomike dhe gjeopolitike, rritja e bashkëpunimeve ndërkombëtare, si dhe kërcënimet kibernetike të sofistikuara, kërkojnë një strategji kombëtare të sigurisë kibernetike dinamike dhe të aftë të përshtatet ndaj ndryshimeve të shpejta në mjedisin digjital.

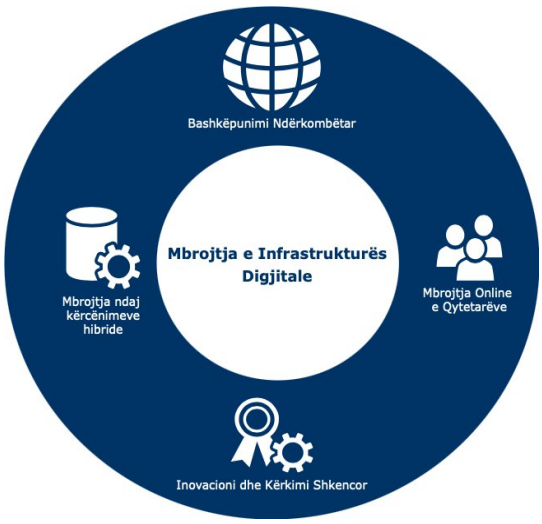

Figura 1. Politikat e Strategjisë

- Strategjia shoqërohet nga një plan veprimi, që përcakton aktivitetet konkrete për implementimin e saj, duke synuar realizimin e objektivave të përcaktuar. Ky plan veprimi specifikon hapa të qartë dhe afate kohore për secilën fazë të procesit.

Qëllimi i politikës 1: **Mbrojtja e infrastrukturës digjitale**: Baza e Strategjisë Kombëtare të Sigurisë Kibernetike është mbrojtja e infrastrukturave kritike dhe të rëndësishme të informacionit në vend, që përfshin rrjetet, sistemet dhe shërbimet, që mbështesin funksionimin e shtetit dhe jetën e përditshme të qytetarëve. Kjo politikë ka për qëllim sigurimin e vazhdimësisë së shërbimeve dhe mbrojtjen e sistemeve të informacionit, që mbajnë në funksion energjinë, transportin, shëndetësinë, financat, administratën publike dhe sektorë të tjerë kyç. Pjesë e kësaj politike janë masat parandaluese dhe mbrojtëse për identifikimin e minimizimin e rreziqeve, si dhe zhvillimi i mekanizmave të reagimit të shpejtë në rastet e incidenteve kibernetike, me qëllim rritjen e qëndrueshmërisë digjitale e kibernetike.

Qëllimi i politikës 2: **Mbrojtja *online* e qytetarëve dhe nxitja e kulturës kibernetike.** Krijimi dhe nxitja e një kulture ndërgjegjësimi për sigurinë kibernetike në të gjitha grupet e shoqërisë janë elemente thelbësore për këtë strategji. Ndërgjegjësimi promovon përgjegjësi të përbashkët. Një qytetar i ndërgjegjshëm kontribuon në një zinxhir më të sigurt në shoqëri, duke minimizuar dobësitë që mund të shfrytëzohen nga sulmuesit. Edukimi dhe ndërgjegjësimi i publikut është një proces i vazhdueshëm, që synon të pajisë qytetarët me njohuri dhe mjete praktike për të adresuar sfidat aktuale dhe për të marrë vendime të informuara. Një shoqëri e informuar ka mundësi të kontribuojë në debatin publik dhe të nxisë për politika më të mira. Po ashtu, është e rëndësishme të promovohet etika kibernetike dhe respektimi i rregullave edukative në internet, si dhe parandalimi i radikalizmit *online*, duke promovuar përdorimin e një gjuhe të respektueshme e të përgjegjshme.

Strategjia Kombëtare e Sigurisë Kibernetike 2025–2030 ka në fokus krijimin e mekanizmave të nevojshëm për mbrojtjen *online* të qytetarëve, veçanërisht mbrojtjen e fëmijëve dhe të të rinjve dhe grupeve të nënpërfaqësuara.

Qëllimi i politikës 3: **Forcimi i bashkëpunimit ndërkombëtar**: Siguria kibernetike është një sfidë ndërkombëtare dhe një përpjekje e përbashkët për të adresuar sfidat, që lidhen me kërcënimet

dhe rreziqet në mjedisin digjital. Strategjia promovon forcimin e bashkëpunimit ndërmjet institucioneve dhe partnerëve ndërkombëtarë, duke nxitur shkëmbimin e informacionit, zhvillimin e kapaciteteve të përbashkëta dhe krijimin e standardeve të unifikuara, duke siguruar një mbrojtje kolektive dhe më efektive kundër kërcënimeve kibernetike. Në këtë kuadër, Shqipëria angazhohet për të kontribuar aktivisht në nismat dhe marrëveshjet ndërkombëtare, veçanërisht në zbatimin me përpikëri të detyrimeve ekzistuese si vend anëtar i NATO-s, duke forcuar kështu qëndrueshmërinë e mjedisit digjital global.

Qëllimi i politikës 4: **Nxitja e inovacionit dhe e kërkimit shkencor**: Strategjia Kombëtare për Sigurinë Kibernetike përqafon përdorimin e teknologjive më të avancuara, përfshirë inteligjencën artificiale, *blockchain* dhe llogaritjen kuantike, për të përforcuar mbrojtjen kibernetike dhe për të adresuar sfidat komplekse të një mjedisi digjital gjithnjë e më të ndërlikuar. Inovacioni është një shtyllë thelbësore që kontribuon në përmirësimin e protokolleve të përparuara të sigurisë, zbulimin e hershëm të kërcënimeve dhe garantimin e qëndrueshmërisë së ekosistemit digjital. Kërkimi shkencor dhe adoptimi i teknologjive të reja rrisin aftësinë strategjike të Shqipërisë për t'u përballur me kërcënimet kibernetike në mënyrë efikase, duke siguruar një mjedis digjital të besueshëm e të qëndrueshëm.

Qëllimi i politikës 5: **Mbrojtja ndaj kërcënimeve hibride**: Për të frenuar kërcënimet hibride të natyrës komplekse, që shfrytëzojnë dobësitë në fushat kibernetike, Shqipëria po harton një strategji mbrojtëse proaktive, të qëndrueshme dhe të përshtatshme. Një nga politikat kyçe të kësaj strategjie është mbrojtja ndaj kërcënimeve hibride. Këto kërcënime përfshijnë aktivitete të dëmshme, që kombinojnë sulme kibernetike me veprime të tjera, si: manipulimi i informacionit, ndikimi ekonomik, manovrat politike, diplomacia shtrënguese dhe kërcënimet ushtarake. Objektivi i kësaj politike është të identifikohen e të neutralizohen kërcënimet hibride përmes forcimit të kapaciteteve mbrojtëse, përmirësimit të bashkëpunimit ndërmjet institucioneve e partnerëve ndërkombëtarë dhe zhvillimit të mekanizmave të shpejtë reagimi, për të ruajtur sigurinë kombëtare dhe integritetin e infrastrukturave kritike e të rëndësishme të informacionit.

Qëllimi i politikës 1: Mbrojtja e infrastrukturës digjitale

Mbrojtja e infrastrukturës digjitale është politika kryesore e Strategjisë Kombëtare për Sigurinë Kibernetike të Shqipërisë 2025–2030. Sigurimi i sistemeve të informacionit, rrjeteve të komunikimit dhe aseteve të infrastrukturës kritike dhe të rëndësishme të informacionit është thelbësor për sigurinë kombëtare, publike dhe stabilitetin ekonomik.

Qëllimi i mbrojtjes së infrastrukturës digjitale synon të krijojë një model të qëndrueshëm dhe efektiv të mbrojtjes së përbashkët, që shpërndan përgjegjësitë dhe menaxhon rrezikun, duke ofruar një nivel të lartë sigurie dhe qëndrueshmërie për ekosistemin digjital.

Adresimi dhe trajtimi i kërcënimeve kibernetike do të jetë i suksesshëm vetëm nëse operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë bashkëpunimin dhe ndërgjegjësimin e nevojshëm për rëndësinë e zbatimit të masave të sigurisë kibernetike.

Në mbështetje të objektivit kryesor të kësaj shtylle për sigurimin dhe mbrojtjen sistemeve të informacionit dhe rrjeteve të komunikimit përmes garantimit të disponueshmërisë, integritetit dhe konfidencialitetit të të dhënave, Shqipëria angazhohet të ndërmarrë nisma të plota dhe të koordinuara, që përfshijnë trajtimin e sfidave në:

- procese;
- teknologji;
- kapacitete njerëzore.

1. Proceset

Proceset luajnë një rol kryesor në Strategjinë Kombëtare për Sigurinë Kibernetike.

Proceset përfshijnë një sërë hapash të ndërlidhur e të koordinuar, që kanë për qëllim mbrojtjen e aseteve digjitale, sistemeve të informacionit dhe rrjeteve të komunikimit nga kërcënimet dhe sulmet kibernetike. Ato përcaktojnë se si një infrastrukturë digjitale ndërvepron me të gjitha aspektet e sigurisë kibernetike, duke përfshirë praktika:

- të qarta dhe të mirëdokumentuara në përcaktimin e roleve e të përgjegjësive;
- dinamika ndaj kërcënimeve hibride;
- të vazhdueshme dhe adoptuese drejt maturitetit të posturës së sigurisë kibernetike të infrastrukturës.

Objektivi specifik 1.1: Hartimi dhe zbatimi i kuadrit ligjor për sigurinë kibernetike

Ky objektiv përfshin procesin e harmonizimit të standardeve dhe direktivave ndërkombëtare në hartimin e legjislacionit dhe të kuadrit rregullator, që përcaktojnë mënyrën e menaxhimit të sigurisë kibernetike në nivel kombëtar. Qëllimi i këtij objektivi është të sigurohet një mbrojtje efektive ndaj kërcënimeve dhe sulmeve kibernetike, duke u përputhur me kërkesat e sigurisë dhe nevojat e zhvillimit të teknologjive të reja.

Objektivi specifik 1.2: Përmirësimi i kapaciteteve monitoruese dhe mbrojtjes së sistemeve

Ky objektiv përfshin monitorimin e vazhdueshëm të sistemeve të informacionit dhe rrjeteve të komunikimit, gjurmimin e aktiviteteve të dyshimta, identifikimin e pikave të dobëta, zhvillimin e produkteve të sigurta *software* dhe *hardware* dhe sigurimin e një qasjeje të sigurt për përdoruesit. Qëllimi i këtij objektivi është minimizimi i rreziqeve përmes implementimit të masave proaktive dhe sigurimit të mbrojtjes së qëndrueshme ndaj sulmeve dhe të kërcënimeve kibernetike, duke përfshirë zgjerimin e aktiviteteve të kontrollit dhe përputhshmërisë për teknologjitë e avancuara, si: *blockchain*, *cloud computing*, AI dhe teknologji të tjera në zhvillim *(emerging technologies),* për të siguruar mbrojtjen e sistemeve të reja dhe integrimin e tyre në ekosistemet ekzistuese të sigurisë.

Objektivi specifik 1.3: Qeverisja kibernetike dhe menaxhimi i rreziqeve

Ky objektiv përfshin vlerësimin e vazhdueshëm të rreziqeve kibernetike, duke përfshirë identifikimin, vlerësimin, analizimin dhe trajtimin e rreziqeve në nivel infrastrukture, sektori dhe kombëtar. Qëllimi i këtij objektivi vë në fokus bashkëpunimin me partnerë kombëtarë dhe ndërkombëtarë për të adresuar rreziqet kibernetike, si dhe për të krijuar kanale komunikimi të shkëmbimit të informacionit.

Objektivi specifik 1.4: Zhvillimi i planeve të reagimit dhe menaxhimit të incidenteve kibernetike

Ky objektiv mbulon menaxhimin dhe shpërndarjen e informacionit lidhur me incidentet kibernetike, inteligjencën e kërcënimeve, analizën e shkaqeve të incidenteve, raportimin për të përmirësuar masat parandaluese dhe reagimin në kohë. Qëllimi është krijimi i proceseve të qarta për trajtimin e incidenteve dhe reagimin e shpejtë për të parandaluar e kufizuar dëmet potenciale në një kohë më të shkurtër.

Objektivi specifik 1.5: Garantimi i transaksioneve elektronike përmes shërbimeve të besuara

Ky objektiv synon garantimin e transaksioneve të sigurta elektronike për bizneset dhe qytetarët nëpërmjet përdorimit të shërbimeve të besuara. Garantimi i sigurisë në përdorimin e mjeteve të identifikimit elektronik dhe shërbimeve të besuara mundëson e lehtëson pjesëmarrjen në mënyrë të sigurt në shoqërinë digjitale, si dhe përdorimin e shërbimeve publike e private *online*.

Objektivi specifik 1.6: Implementimi i skemës së certifikimit të sigurisë kibernetike

Ky objektiv synon krijimin e një mekanizmi kombëtar të besueshëm për certifikimin e sigurisë kibernetike, të harmonizuar me kuadrin ligjor të Bashkimit Evropian. Përmes përdorimit të produkteve, shërbimeve dhe proceseve TIK të certifikuara, do të rritet besueshmëria në tregun digjital, do të garantohet një nivel më i lartë sigurie për produktet, shërbimet e proceset TIK, si dhe do të forcohet mbrojtja dhe qëndrueshmëria e infrastrukturave kritike dhe të rëndësishme të informacionit.

2. Kapacitetet njerëzore

Përmbushja e vizionit dhe e qëllimit të Strategjisë Kombëtare kërkon zhvillimin e aftësive, të njohurive dhe të kulturës së duhur në fushën e sigurisë kibernetike. Kapacitet njerëzore luajnë një rol të rëndësishëm në rritjen e nivelit të sigurisë kibernetike, duke aplikuar ekspertizën e tyre në projektimin dhe implementimin e masave të sigurisë. Ky proces përfshin të gjithë aktorët si politikëbërësit, specialistët e sigurisë kibernetike dhe përdoruesit e sistemeve digjitale, të cilët duhet

të kuptojnë rolet e përgjegjësitë për të menaxhuar e zvogëluar rreziqet dhe duke kontribuar në rritjen e qëndrueshmërisë së sigurisë kibernetike. Programet e edukimit, trajnimit dhe ndërgjegjësimit janë thelbësore për forcimin e kapaciteteve njerëzore, duke mundësuar krijimin e një mjedisi digjital të sigurt.

Objektivi specifik 2.1: Promovimi dhe zhvillimi i kulturës kibernetike

Forcimi i kulturës së sigurisë kibernetike është thelbësor për mbrojtjen e rrjeteve dhe të sistemeve të informacionit, pasi përdoruesit shpesh janë hallka më e dobët e zinxhirit të mbrojtjes. Ky objektiv kërkon trajnime të vazhdueshme, fushata ndërgjegjësimi dhe partneritete me median dhe organizatat e komunitetit. Krijimi i mjediseve proaktive dhe përmirësimi i vazhdueshëm i praktikave janë të domosdoshme për të siguruar qëndrueshmëri digjitale e kibernetike. Po ashtu, përfshirja e të gjitha grupeve të interesit dhe zbatimi i parimeve të sigurisë në të gjitha nivelet kontribuojnë në forcimin e sigurisë kibernetike.

Objektivi specifik 2.2: Rritja e kapaciteteve profesionale

Zhvillimi i kapaciteteve profesionale nëpërmjet integrimit të kurrikulave të përmirësuara në sektorin arsimor, trajnimeve të specializuara, certifikimeve profesionale, tërheqjes dhe angazhimit të talenteve, gjithëpërfshirjes dhe bashkëpunimit me organizatat ndërkombëtare për praktikat më të mira synon krijimin e një qasjeje efektive në adresimin e sfidave dhe përballimin e rreziqeve të sigurisë kibernetike në nivel kombëtar.

3. Teknologjia

Teknologjia luan një rol të rëndësishëm në mbrojtjen e infrastrukturës digjitale, pasi ajo ofron mjetet dhe burimet e nevojshme për implementimin e masave të sigurisë kibernetike për parandalimin e menaxhimin e kërcënimeve kibernetike. Avancimi i teknologjisë shton nevojën për një reagim të shpejtë ndaj sulmeve kibernetike, gjithmonë e më të sofistikuara. Ky proces përfshin një sërë sfidash të mëdha për të siguruar një mbrojtje të qëndrueshme dhe efikase kundër këtyre kërcënimeve komplekse.

Objektivi specifik 3.1: Përdorimi dhe integrimi i teknologjive të avancuara

Përdorimi dhe integrimi i teknologjive të avancuara, si inteligjenca artificiale (**AI**), programet kompjuterike inteligjente (**LLM**), kompjuterat kuantikë, kriptografia kuantike dhe teknologjitë e decentralizuara ***(blockchain)*** do të përmirësojnë sigurinë kibernetike, duke mundësuar identifikimin e avancuar të kërcënimeve dhe reagimeve të automatizuara.

Objektivi specifik 3.2: Monitorimi, zbulimi dhe mbrojtja kibernetike, duke shfrytëzuar teknologjitë e avancuara

Shqipëria angazhohet të sigurojë një nivel të qëndrueshmërisë kibernetike proporcional me rrezikun, duke zgjeruar kapacitetet teknologjike të monitorimit, për të identifikuar, parandaluar e trajtuar kërcënimet kibernetike në të gjitha infrastrukturat kritike dhe të rëndësishme të informacionit.

Objektivi specifik 3.3: Implementimi i kornizës "secure by design" për infrastrukturat digjitale

Zbatimi i parimit *"secure by design"* integron masat e sigurisë kibernetike në të gjitha fazat e ciklit të jetës së sistemeve dhe shërbimeve digjitale, blerje dhe çaktivizimi të sigurt. Kjo qasje do të sigurojë një proces të vazhdueshëm dhe interaktiv për menaxhimin e rrezikut, me përfshirjen e politikave, procedurave dhe ekspertizës të sigurisë në çdo fazë të zhvillimit të shërbimeve digjitale.

Objektivi specifik 3.4: Menaxhimi efektiv i teknologjive të vjetruara

Kjo qasje do të sigurojë një menaxhim efektiv të teknologjive të vjetruara në nivel kombëtar përmes zhvillimit dhe zbatimit të politikave gjithëpërfshirëse, që synojnë identifikimin, përditësimin, izolimin ose zëvendësimin e tyre, duke kontribuar në forcimin e mbrojtjes kibernetike, qëndrueshmërinë e shërbimeve dhe rritjen e besueshmërisë së infrastrukturave kritike dhe të rëndësishme të informacionit.

Objektivi specifik 3.5: Përdorimi i teknologjive alternative kompensuese për sigurinë kibernetike

Shqipëria do të promovojë dhe do të implementojë teknologji alternative me burim të hapur *(open-source)*. Si një masë mbështetëse do të zbatohet në rastet kur teknologjitë me burim të mbyllur nuk janë të disponueshme ose të përballueshme për infrastrukturat kritike dhe të rëndësishme të informacionit (OIKI/OIRI). Kjo qasje synon të garantojë vazhdimësinë e mbrojtjes kibernetike dhe ruajtjen e qëndrueshmërisë operacionale të këtyre infrastrukturave, veçanërisht në kushte të kufizuara teknologjike ose financiare.

Qëllimi i politikës 2: Mbrojtja *online e qytetarëve* dhe nxitja e kulturës kibernetike

Kjo politikë synon të sigurojë një qasje gjithëpërfshirëse për mbrojtjen *online* dhe promovimin e një kulture të qëndrueshme kibernetike në Shqipëri. Ajo përqendrohet në përshtatshmërinë e kuadrit ligjor, duke siguruar që të gjithë qytetarët, përfshirë grupet e nënpërfaqësuara, janë të mbrojtur dhe kanë mundësi të barabarta për pjesëmarrje në hapësirën kibernetike. Për të arritur këtë qëllim, organizohen tavolina të rrumbullakëta, ku përfaqësues nga institucionet publike, sektori privat, organizatat jofitimprurëse (OJF), media dhe shoqëria civile diskutojnë sfidat dhe zgjidhjet për sigurinë kibernetike. Këto platforma dialogu ndihmojnë në krijimin e politikave të bazuara në konsensus dhe adresimin e nevojave të ndryshme të komuniteteve. Gjithashtu, aktivitetet dhe trajnimet për rritjen e ndërgjegjësimit dhe aftësive kibernetike janë prioritet, ku përfshihen fushata ndërgjegjësimi për rreziqet *online*, programe edukative për të rinjtë dhe grupet e nënpërfaqësuara, si dhe trajnime specifike për profesionistët dhe publikun e gjerë. Bashkëpunimi ndërinstitucional dhe ndërsektorial luan një rol të rëndësishëm në zbatimin e kësaj politike. Institucionet publike, sektori privat, OJF-të dhe media bashkërendojnë përpjekjet për të ndërtuar një ekosistem të fortë të sigurisë kibernetike, duke garantuar një qasje gjithëpërfshirëse dhe të qëndrueshme për mbrojtjen e nxitjen e qytetarëve.

Objektivi specifik 1: Hartimi dhe zhvillimi i Planit Kombëtar për Ndërgjegjësimin e Qytetarëve (PKNQ)

Ky objektiv synon hartimin dhe zbatimin e një plani gjithëpërfshirës për ndërgjegjësimin e qytetarëve lidhur me sfidat e rreziqet, që lidhen me sigurinë kibernetike, si dhe përfitimet e të qenët pjesë e një mjedisi digjital të sigurt. PKNQ-ja do të përfshijë fushata të organizuara në institucione arsimore, institucione publike, dhe komunitete lokale, me qëllim rritjen e ndërgjegjësimit mbi praktikat më të mira për sigurinë *online*. Në këtë kuadër, do të zhvillohen programe edukative, që synojnë të pajisin qytetarët me aftësi të domosdoshme për të identifikuar e shmangur kërcënimet kibernetike, duke përfshirë mbrojtjen nga krimet e mundshme kibernetike, përfshirë mashtrimet, vjedhjen e identitetit etj., duke krijuar një zinxhir edukimi të vazhdueshëm për të gjithë.

Objektivi specifik 2: Hartimi i një kornize ligjore për qasjen gjithëpërfshirëse të qytetarëve

Ky objektiv synon krijimin dhe përshtatjen e një kuadri ligjor të avancuar, i cili garanton që të gjithë qytetarët të kenë akses të barabartë në hapësirën digjitale. Korniza ligjore do të përfshijë mekanizma, që rregullojnë transparencën, barazinë në aksesin ndaj shërbimeve digjitale dhe mbrojtjen nga diskriminimi *online*. Për të arritur këtë, do të organizohen konsultime gjithëpërfshirëse me qytetarët, institucionet publike, sektorin privat dhe OJF-të, për të siguruar që zëri i të gjithëve reflektohet në politikat dhe legjislacionin përkatës.

Objektivi specifik 3: Krijimi i mekanizmave të nevojshëm për mbrojtjen online të fëmijëve

Fëmijët përbëjnë një nga kategoritë më të cenueshme në ekosistemin digjital, ndaj ky objektiv synon krijimin dhe zbatimin e mekanizmave specifikë për garantimin e sigurisë së tyre *online*. Në këtë kuadër, do të zhvillohen platforma të dedikuara, që ofrojnë përmbajtje edukative dhe argëtuese në një mjedis të sigurt e të monitoruar, ndërsa do të implementohen sisteme të avancuara monitorimi dhe plane të përbashkëta ndërinstitucionale për të mbështetur prindërit dhe kujdestarët në mbikëqyrjen efektive të aktiviteteve digjitale të fëmijëve. Si pjesë e këtij objektivi, do të realizohen, gjithashtu, fushata të strukturuara ndërgjegjësimi dhe programe trajnuese, duke i pajisur ata me aftësitë e nevojshme për të identifikuar e adresuar rreziqet kibernetike. Kjo qasje

gjithëpërfshirëse synon krijimin e një mjedisi digjital të sigurt dhe edukativ, që promovon mirëqenien dhe zhvillimin e fëmijëve.

Objektivi specifik 4: Nxitja e barazisë gjinore në hapësirën digjitale

Ky objektiv ka për qëllim krijimin e një mjedisi digjital gjithëpërfshirës dhe të sigurt për gratë dhe vajzat, duke u fokusuar në fuqizimin e tyre dhe luftimin e çdo forme diskriminimi ose dhune kibernetike. Zbatimi i këtij objektivi është i lidhur ngushtë me adresimin e një sërë sfidash, që ndikojnë në pjesëmarrjen e barabartë të grave dhe të vajzave në sektorin digjital, përfshirë:

- pabarazitë në akses dhe përdorim të teknologjive digjitale, ku gratë dhe vajzat përballen me mundësi të kufizuara krahasuar me burrat dhe djemtë;

- ndarjen gjinore në fushat e edukimit, veçanërisht në shkencë, teknologji, inxhinieri dhe matematikë (*STEM*), ku vajzat kanë më pak gjasa të ndjekin apo të përfaqësohen në këto disiplina;

- pjesëmarrjen e ulët të grave në tregun digjital të punës, duke përfshirë përfaqësimin e tyre të kufizuar në karriera në fushën e teknologjisë së informacionit e të komunikimit (TIK);

- dhunën dhe ngacmimet në internet, përfshirë bullizmin dhe format e tjera të dhunës me bazë gjinore, që kufizojnë pjesëmarrjen aktive të grave dhe vajzave në mjedisin *online*;

- përforcimin e roleve stereotipike gjinore dhe promovimin e normave të dëmshme gjinore në internet, të cilat kontribuojnë në pabarazi;

- mungesën e të dhënave administrative të ndara sipas gjinisë, si dhe boshllëqet në koordinimin ndërinstitucional për përcaktimin dhe monitorimin e treguesve kyç gjinorë.

Përmes fushatave ndërgjegjësuese, do të promovohet pjesëmarrja aktive e grave dhe vajzave në sektorin e teknologjisë dhe sigurisë kibernetike. Aktivitetet do të përfshijnë trajnime për fuqizimin e tyre përmes aftësive digjitale, krijimin e platformave të sigurisë, që adresojnë ngacmimet *online,* si dhe zhvillimin e rrjeteve mbështetëse për gratë profesioniste në fushën e teknologjisë. Ky objektiv do të synojë, gjithashtu, krijimin e politikave, që inkurajojnë barazinë gjinore në çdo aspekt të hapësirës digjitale dhe promovojnë një kulturë mbështetëse për gratë dhe vajzat *online.*

Objektivi specifik 5: Krijimi i mekanizmave të duhur për mbrojtjen e* SME-ve *online

Brenda përpjekjeve për të forcuar sigurinë digjitale dhe për të përmirësuar qëndrueshmërinë kibernetike të sektorit privat, një fokus i veçantë i është kushtuar promovimit të edukimit në fushën e teknologjisë dhe sigurisë kibernetike te ndërmarrjet e vogla dhe të mesme (SME). Kjo nismë synon të rrisë ndërgjegjësimin dhe të forcojë kapacitetet mbrojtëse të SME-ve, duke u mundësuar atyre të përballen më mirë me sfidat në rritje, që lidhen me kërcënimet kibernetike. Në këtë drejtim, do të hartohen udhëzime praktike për masat e nevojshme të sigurisë kibernetike, të cilat do të shërbejnë si burime orientuese për SME-të në përmirësimin e infrastrukturës së tyre digjitale dhe në zbatimin e praktikave më të mira për mbrojtjen e të dhënave dhe sistemeve të tyre. Gjithashtu, do të organizohen trajnime vjetore të dedikuara për punonjësit e SME-ve, me qëllim zhvillimin e aftësive të tyre praktike në identifikimin dhe menaxhimin e rreziqeve kibernetike. Këto trajnime do të ofrojnë njohuri të specializuara në fushat thelbësore të sigurisë digjitale dhe do të kontribuojnë në krijimin e një kulture më të fortë sigurie brenda sektorit të SME-ve.

Objektivi specifik 6: Krijimi i mekanizmave të nevojshëm për mbrojtjen dhe fuqizimin e grupeve të nënpërfaqësuara

Ky objektiv synon të mbrojë dhe të fuqizojë grupet e nënpërfaqësuara, duke krijuar platforma gjithëpërfshirëse, që adresojnë nevojat specifike të këtyre grupeve, për garantimin në një qasje të barabartë në mjetet dhe shërbimet digjitale. Përmes programeve edukative dhe trajnimeve, këto grupe do të fuqizohen për të qenë më aktive dhe të mbrojtura në hapësirën digjitale. Gjithashtu, do të implementohen politika dhe mekanizma, që adresojnë diskriminimin *online* dhe sigurojnë një mjedis digjital të barabartë e gjithëpërfshirës për të gjithë. Ky objektiv do të realizohet përmes bashkëpunimit të ngushtë me organizatat, që mbështesin këto grupe, institucionet publike dhe sektorin privat.

Qëllimi i politikës 3: Forcimi i bashkëpunimit ndërkombëtar

Siguria kibernetike është një sfidë ndërkombëtare dhe një përpjekje e përbashkët për të adresuar sfidat, që lidhen me kërcënimet e rreziqet në mjedisin digjital. Strategjia promovon forcimin e bashkëpunimit ndërmjet institucioneve dhe partnerëve ndërkombëtarë, duke nxitur shkëmbimin e informacionit, zhvillimin e kapaciteteve të përbashkëta dhe krijimin e standardeve të unifikuara, duke siguruar një mbrojtje kolektive dhe më efektive kundër kërcënimeve kibernetike. Në këtë kuadër, Shqipëria angazhohet për të kontribuar aktivisht në nismat e në marrëveshjet ndërkombëtare për sigurinë kibernetike, duke forcuar kështu qëndrueshmërinë e mjedisit digjital global.

Objektivi specifik 1: Harmonizimi i politikave dhe legjislacionit

Qëllimi i këtij objektivi është të sigurohet përputhshmëria e legjislacionit të sigurisë kibernetike të Shqipërisë me standardet dhe rregulloret ndërkombëtare, duke krijuar një kornizë ligjore të fortë dhe të qëndrueshme. Ky harmonizim do të mundësojë një reagim më efikas dhe të koordinuar ndaj kërcënimeve kibernetike, duke rritur mbrojtjen e hapësirës digjitale dhe kontributin e Shqipërisë në nivel global. Sulmet kibernetike janë më komplekse dhe, nisur nga këto kushte menaxhimi, parandalimi apo rimëkëmbja pas tyre duhet të bazohet në pesë elemente shumë të rëndësishme, si: ligjore, teknike, organizative, kapacitet profesional dhe bashkëpunimi. Duke qenë se natyra e këtyre sulmeve ka treguar se nuk varen nga kufijtë ndërmjet shteteve, situata ekonomike, politike apo sociale, legjislacioni apo standardet e unifikuara janë prioritet në luftën e përbashkët kundër sulmeve të vazhdueshme kibernetike.

Objektivi specifik 2: Forcimi i bashkëpunimit rajonal (WB6) dhe ndërkombëtar

Për të ndërtuar një ekosistem digjital të sigurt e të qëndrueshëm, nuk mund të veprosh i vetëm, pasi sulmet kibernetike apo ato hibride kanë treguar se praktika më e mirë kundër tyre është bashkëpunimi. Edhe kur një shtet është objektivi kryesor i aktorëve keqdashës, pasojat e sulmeve kibernetike shtrihen përtej kufijve të tij, duke ndikuar nivelin rajonal dhe më tej. Kjo e bën bashkëpunimin ndërkombëtar një domosdoshmëri për të përballuar kërcënimet kibernetike, për të ndërmarrë të gjitha masat për parandalimin e ndikimit të tyre në hapësirën e përbashkët digjitale. Zhvillimi dhe forcimi i bashkëpunimit rajonal e ndërkombëtar për të përballuar kërcënimet kibernetike mund të arrihet duke përmirësuar shkëmbimin e informacionit dhe koordinimin e përgjigjeve ndaj incidenteve kibernetike.

Objektivi specifik 3: Zhvillimi i diplomacisë kibernetike

Zhvillimi i diplomacisë kibernetike, me qëllim krijimin e kornizave të qarta diplomatike në nivel kombëtar e ndërkombëtar për të adresuar efektivisht çështjet e sigurisë kibernetike, duke angazhuar shtetet, organizatat ndërkombëtare dhe aktorët e tjerë në mbrojtjen e infrastrukturave digjitale dhe sistemeve të informacionit.

Qëllimi i politikës 4: Nxitja e inovacionit dhe kërkimit shkencor në sigurinë kibernetike

Shqipëria synon të zhvillojë një ekosistem të qëndrueshëm përmes inovacionit dhe kërkimit shkencor, duke theksuar bashkëpunimin ndërmjet institucioneve të arsimit të lartë, sektorit privat dhe institucioneve publike në rritjen e kapaciteteve kombëtare në fushën e sigurisë kibernetike dhe krijimin e zgjidhjeve të reja teknologjike. Kjo qasje forcon aftësinë për t'u përballur me sfidat kibernetike, por edhe ndihmon në krijimin e një mjedisi inovativ dhe të sigurt digjital për Shqipërinë.

Objektivi specifik 1: Ngritja e Qendrës Kombëtare të Ekselencës për Sigurinë Kibernetike

Krijimi i Qendrës Kombëtare të Ekselencës për Sigurinë Kibernetike (QKESK) si një qendër inovative për kërkim dhe zhvillim teknologjik do të mundësojë bashkëpunimin e ngushtë ndërmjet institucioneve të arsimit të lartë, qendrave kërkimore kombëtare e ndërkombëtare dhe institucioneve publike e private. Ajo do të nxisë kërkimin shkencor, identifikimin e talenteve dhe trajnimin e tyre me teknologjitë më të avancuara. Në fokus do të jetë zhvillimi i zgjidhjeve inovatore, si inteligjenca artificiale, analiza e të dhënave dhe kriptografia, për parandalimin dhe zbulimin e sulmeve kibernetike në kohë reale, me synimin për të forcuar sigurinë dhe qëndrueshmërinë digjitale kombëtare.

Objektivi specifik 2: Mbështetja e startup-eve në fushën e sigurisë kibernetike

Ky objektiv synon të mbështesë zhvillimin e *startup*-eve në fushën e sigurisë kibernetike përmes krijimit të një mjedisi që nxit inovacionin dhe sipërmarrjen teknologjike. Kjo përfshin lehtësimin e aksesit në burime kërkimore dhe ekspertizë teknike, ofrimin e trajnimeve të specializuara dhe programeve të mentorimit, si dhe nxitjen e bashkëpunimit ndërmjet sektorit publik, privat dhe institucioneve të arsimit të lartë. Një fokus i veçantë do t'i kushtohet nxitjes së pjesëmarrjes së grave dhe vajzave në sektorin e sigurisë kibernetike.

Objektivi specifik 3: Zhvillimi i programeve të financimit për kërkim dhe inovacion në sigurinë kibernetike

Të zhvillohen programe financimi për kërkimin dhe inovacionin në sigurinë kibernetike. Këto programe do të përfshijnë krijimin e fondeve specifike, promovimin e barazisë gjinore në politikat e inovacionit e të kërkimit shkencor, ofrimin e stimujve fiskalë për bizneset, që investojnë në teknologji të sigurta dhe promovimit të partneriteteve publike-private për bashkëfinancimin e projekteve inovative.

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.

Objektivi specifik 1: Hartimi i kuadrit ligjor për mbrojtjen ndaj kërcënimeve kibernetike hibride

Hartimi i një kuadri ligjor të përshtatshëm për mbrojtjen ndaj kërcënimeve kibernetike hibride do të mundësojë parandalimin, identifikimin dhe menaxhimin e kërcënimeve. Ky kuadër ligjor do të sigurojë një bashkëpunim të ngushtë ndërinstitucional kombëtar e ndërkombëtar, duke forcuar mbrojtjen e infrastrukturave ndaj kërcënimeve hibride.

Objektivi specifik 2: Koordinimi ndërinstitucional dhe ndërkombëtar për mbrojtjen ndaj kërcënimeve hibride

Bashkëpunimi dhe koordinimi ndërinstitucional e ndërkombëtar do të adresojë kërcënimet hibride dhe do të optimizojë ndarjen e informacionit dhe të burimeve. Koordinimi i ngushtë siguron një reagim të shpejtë dhe efikas për të parandaluar e menaxhuar pasojat e kërcënimeve hibride.

Objektivi specifik 3: Krijimi i mekanizmave të mbrojtjes ndaj kërcënimeve hibride

Për zhvillimin e një strukture të integruar dhe efikase për parashikimin, identifikimin dhe reagimin ndaj kërcënimeve hibride, që përfshijnë sulme kibernetike dhe dezinformim, është i nevojshëm përdorimi i mjeteve dhe i teknologjive moderne. Platformat për shkëmbimin e informacionit, si dhe rritja e ndërgjegjësimit në publik për të siguruar reagim të shpejtë dhe efektiv ndaj kërcënimeve ruan stabilitetin e sigurinë kombëtare.

Objektivi specifik 4: Krijimi i mekanizmave për parandalimin dhe hetimin e krimit kibernetik

Parandalimi i krimit kibernetik kërkon një qasje proaktive dhe të bazuar në teknologji të avancuar, që përfshin zbulimin e hershëm dhe reagimin e shpejtë ndaj kërcënimeve. Ky objektiv synon krijimin e një mjedisi të sigurt dhe të qëndrueshëm në hapësirën digjitale, duke parandaluar e menaxhuar efektet e mundshme të krimeve kibernetike.

Zbatimi, përgjegjësia e institucioneve, llogaridhënia

Hartimi i Strategjisë Kombëtare të Sigurisë Kibernetike 2025–2030 mbështetet në vendimin nr. 783, datë 18.12.2024, të Këshillit të Ministrave, "Për organizimin dhe funksionimin e Autoritetit Kombëtar për Sigurinë Kibernetike", si dhe në angazhimet e në standardet e Bashkimit Evropian dhe organizmave të tjerë ndërkombëtarë.

- Angazhimi i institucioneve publike dhe private i jep kësaj strategjie mundësinë për të qenë objektive dhe e realizueshme. Grupi ndërinstitucional i punës, si dhe të gjithë aktorët e përfshirë në konsultime dhanë komente të vlefshme, duke e rishikuar disa herë draftin e përgatitur, me qëllim miratimin e një strategjie gjithëpërfshirëse, ku secili të gjejë veten e të japë kontributin e tij në garantimin e sigurisë kibernetike të vendit.

- Kjo strategji nuk është një strategji vetëm për institucionet, por është një strategji, që nxit dhe mbështet mbrojtjen kibernetike edhe të individit, qytetarëve dhe, veçanërisht, fëmijëve si e ardhmja e këtij vendi. Në të evidentohen edhe masa për të luftuar jo vetëm krimin kibernetik, por edhe nxitjen e terrorizmit e të ekstremizmit të dhunshëm nëpërmjet hapësirës kibernetike.

Plani i veprimit, që shoqëron Strategjinë Kombëtare të Sigurisë Kibernetike 2025–2027, u përgatit, bazuar në:

a) Strategjinë Kombëtare për Sigurinë Kibernetike 2025–2030 dhe politikat përbërëse të saj;

b) planet buxhetore të institucioneve publike.

Sikurse paraqitet edhe në objektivat specifikë dhe në aktivitetet kryesore të propozuara në këtë strategji dhe në planin e veprimit, rolin koordinues duhet ta kryejë Autoriteti Kombëtar për Sigurinë Kibernetike. Gjithashtu, në këtë dokument janë marrë parasysh detyrimet, që lindin nga procesi i integrimit evropian dhe përshtatja me direktivat NIS2, EIDAS2, si dhe angazhimet si vend anëtar i NATO-s.

Të gjitha masat/aktivitetet e propozuara, pasi u vlerësuan dhe plotësuan edhe nga grupi ndërinstitucional i punës, përgjegjës për hartimin e strategjisë u detajuan më tej gjatë vlerësimit të efekteve financiare për zbatimin e kësaj strategjie kombëtare dhe planit të saj të veprimit 2025–2027, me nevojën për rishikim periodik, bazuar në dinamikën e zhvillimit në fushën e sigurisë kibernetike.

Secili institucion përgjegjës për aktivitetet duhet të planifikojë realizimin e tyre, duke garantuar buxhetet e planifikuara, burimet njerëzore dhe kapacitetet teknike, me qëllim realizimin e tyre. Çdo vit do të bëhet vlerësimi i zbatimit të aktiviteteve dhe arritjes së objektivave të identifikuar nëpërmjet realizimit të indikatorëve. Institucionet përgjegjëse për realizimin e aktiviteteve dhe arritjes së rezultateve kanë detyrimin e raportimit sipas standardeve raportuese. Koordinatori i Strategjisë duhet të përgatitë raportin vjetor dhe ta publikojë atë.

Plani i veprimit dhe burimet financiare për zbatim

Metodologjia e kostimit të aktiviteteve

Shpenzimet e nevojshme për zbatimin e PKV-së janë nxjerrë duke kostuar secilin nga aktivitetet e këtij plani veprimi. Metodologjia e zbatuar për llogaritjen e kostove paraqet një kombinim të metodave, që mund të përdoren në rastet e strategjive me shumë aktorë. Metodologjia kryesore e përdorur është kostimi i bazuar në aktivitete *(Activity Based Costing-ABC),* ku, për çdo aktivitet, evidentohet institucioni përgjegjës, si dhe burimi i mbulimit të kostove dhe alokohen burimet për të gjitha produktet dhe shërbimet në bazë të konsumit aktual për secilin aktivitet.

Buxheti u hartua mbështetur në koston e secilit aktivitet të pasqyruar në planin e veprimit, kohështrirjen dhe frekuencën e zbatimit të tij, si dhe numrin e përfituesve për aktivitete të caktuara. Për llogaritjen e shpenzimeve për aktivitetet kryesore është vepruar, si më poshtë:

- Llogaritja e shpenzimeve për burime njerëzore bazohet në kohën e parashikuar për realizimin e veprimtarisë dhe një pagë mesatare ditore të një kategorie të caktuar.

- Llogaritja e shpenzimeve për shërbime. Për këto aktivitete janë mbajtur parasysh kostot e shërbimeve të institucioneve përkatëse, bazuar në standardet e miratuara.

- Llogaritja e shpenzimeve për aktivitete, që lidhen me hartimin e rishikimin e legjislacionit, monitorimin dhe funksionimin e strukturave të përhershme etj. Për këto aktivitete, gjatë llogaritjeve, janë mbajtur parasysh shpenzimet e vazhdueshme, që do të ndodhin, për shembull, për pagat, kontributet e sigurimeve shoqërore, ekspertizën e huaj (kur është parashikuar në plan) dhe mjetet konsumi.

- Llogaritja e shpenzimeve për aktivitete, që lidhen me studime, fushata ndërgjegjësuese, programe trajnimi, ekspertiza të huaja etj. Llogaritja e kostove është bërë sipas iniciativave specifike të ngjashme, si dhe sipas natyrës së aktiviteteve dhe kostove, që ofron tregu për shërbime të tilla.

- Në llogaritjen e shpenzimeve për trajnime është mbajtur në konsideratë kostoja e trajnimit për një person. Si kosto për njësi janë përdorur kostot e aplikuara për trajnime të ngjashme në të shkuarën.

- Për atë pjesë të aktiviteteve, ku informacioni nuk është i plotë (si në rastin e projekteve apo të studimeve), është ndjekur metoda e vlerësimit për analogji ose janë marrë në konsideratë shpenzimet e bëra për aktivitete të ngjashme, që kanë qenë përfshirë në planet buxhetore të mëparshme.

Buxheti dhe burimet financiare për zbatimin e planit të veprimit

Strategjia Kombëtare e Sigurisë Kibernetike do të zbatohet në periudhën 2025–2030. Për të mundësuar zbatimin e saj, janë llogaritur shpenzimet e nevojshme për zbatimin e secilit aktivitet, objektiv specifik dhe qëllim të politikave. Buxheti i përgjithshëm për zbatimin e Strategjisë është reflektuar në disa forma:

- Buxheti i përgjithshëm sipas viteve për secilin aktivitet, objektiv specifik, qëllim strategjik dhe burime të financimit;
- Buxheti i detajuar sipas aktiviteteve, burimeve të financimit dhe institucioneve përgjegjëse.