|  |
| --- |
| **RAPORTI I VLERËSIMIT TË NDIKIMIT** |
| **EMËRTIMI I PROPOZIMIT TË POLITIKËS**  | Projektligj “Për Sigurinë Kibernetike” |
| **MINISTRIA UDHËHEQËSE**  | Kryeministria/   |
| **FAZA E POLITIKËS/VLERËSIMIT TË NDIKIMIT** | Zhvillim |
| **BURIMI I PROPOZIMIT TË POLITIKËS** | Transpozim i Direktivës së BE -së |
| **DIREKTIVË/RREGULLORE E BE-së**  | Direktiva e BE-së nr.2022/2555 të Parlamentit dhe Këshillit Evropian , datë 14 dhjetor 2022 “Mbi masat për një nivel të lartë të përbashkët të sigurisë kibernetike në të gjithë Bashkimin Evropian, duke ndryshuar Rregulloren (BE) nr.910/2014 dhe Direktivën (BE) nr. 2018/1972, dhe duke shfuqizuar Direktivën (BE) nr. 2016/1148 me efekt prej 18 tetorit 2024, NIS 2. |
| **PUBLIKIMET DHE STRATEGJITË E LIDHURA** | Vendim i Këshillit të Ministrave nr.1084 datë 24.12.2020 "Për miratimin e Strategjisë Kombëtare për Sigurinë Kibernetike dhe të planit të veprimit 2020 – 2025"Programi Qeverisës 2021-2025. |
|  **DATA E KONSULTIMIT PUBLIK** | 26.04.2023 |
| **DATA E VLERËSIMIT TË NDIKIMIT**  | 26/04/2023 |
| **A E KA SHQYRTUAR KRYEMINISTRIA VLERËSIMIN E NDIKIMIT?** **NËSE PO, JEPNI DATËN E SHQYRTIMIT** | Po  |
| **NUMRI I VLERËSIMIT TË NDIKIMIT** | 2023–AKCESK – Nr. 1 VN  |
| **TE DHËNA KONTAKTI** **(EMRI, E-MAIL, NUMRI I TELEFONIT TË PERSONIT TË KONTAKTIT)** |  Oltjana Beci+35542221039oltjana.beci@cesk.gov.alAnxhela Brahimi+35542221039anxhela.brahimi@cesk.gov.al  |
| **PJESA 1: PËRMBLEDHJE EKZEKUTIVE (maksimumi 2 faqe)** |
| **PËRKUFIZIMI I PROBLEMIT***Cili është problemi në shqyrtim dhe cilat janë shkaqet e tij? Jepni arsyet e nevojës së ndërhyrjes së qeverisë. (jo më shumë se 10 rreshta)*  Problemi lidhet me nevojën për të përmirësuar dhe shtuar mekanizmat e duhur dhe të përshtatshëm me qëllim forcimin e sigurisë kibernetike në vend. Rrjetet dhe sistemet e informacionit luajnë një rol të rëndësishëm në shoqërinë shqiptare. Shkalla, shpeshtësia dhe ndikimi i incidenteve të sigurisë janë në rritje dhe përfaqësojnë një shqetësim dhe kërcënim serioz për funksionimin e rrjeteve dhe sistemeve të informacionit, dhe rrjedhimisht edhe të vetë funksionimit të shtetit. Kapacitetet e deritanishme nuk janë të mjaftueshme për të garantuar një nivel të lartë sigurie në rrjetet dhe sistemet e informacionit. Përgatitja e përgjigjeve ndaj sulmeve apo incidenteve kibernetike nuk mjafton në nivelin që ato paraqiten, dhe kjo çon në domosdoshmërinë e ngritjes së kapaciteteve të reja teknike dhe ligjore.Për një përgjigje sa më efektive ndaj sfidave të sigurisë kibernetike është e nevojshme një qasje gjithëpërfshirëse në nivel shtetëror dhe më gjerë në nivel ndërkombëtar, që do të përfshinte krijimin e kapaciteteve të nevojshme me qëllim planifikimin, shkëmbimin e informacionit, bashkëpunimin dhe detyrimet e përbashkëta të sigurisë për operatorët e infrastrukturave të informacionit. Shihet i nevojshëm angazhimi i qeverisë në zgjerimin e fushëveprimit dhe masave për rritjen e nivelit të sigurisë kibernetike. Po ashtu nevojitet ndërhyrja e qeverisë për krijimin ose përmirësimin e strukturave dhe mekanizmave për të garantuar sigurinë kibernetike, trajtuar dhe menaxhuar incidentet kibernetike, si dhe për të menaxhuar emergjencat apo krizën kibernetike në nivel kombëtar. Disa nga shkaqet kryesore të identifikuara mund të përmblidhen si më poshtë:  * Mungesa e parashikimeve të qarta ligjore lidhur me subjektet përgjegjëse të sigurisë kibernetike dhe detyrat përkatëse të tyre (CSIRT Kombëtar, CSIRT Sektorial, dhe CSIRT pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit).
* Mungesa e parashikimeve në kuadrin ligjor për ngritjen e një strukture që bën monitorimin e sigurisë kibernetike në nivel kombëtar.
* Mungesa e parashikimeve ligjore lidhur me trajtimin e gjendjes së situatave emergjente, krizës kibernetike si dhe strukturave përkatëse për menaxhimin e tyre (CERT).
* Mungesa e parashikimeve ligjore përsa i përket hartimit dhe monitorimit të Strategjisë Kombëtare të Sigurisë Kibernetike.

• Mungesa e dispozitave lidhur me certifikimin e sigurisë kibernetike dhe procedurat përkatëse.* Mungesa e parashikimeve të qarta ligjore lidhur me administrimin e sigurisë kibernetike (masat e sigurisë, masat për menaxhimin e riskut, raportimin e incidenteve kibernetike).

Plotësimi i kuadrit rregullator në këtë drejtim është detyrim i vendit edhe në kuadër të procesit të integrimit evropian. Plani Kombëtar i Integrimit Evropian të Republikës së Shqipërisë (2023-2025) ka parashikuar transpozimin e Direktivës së BE-së nr.2016/1148, si dhe të Direktivës nr.2022/2555. |
| **OBJEKTIVAT***Cilat janë objektivat dhe rezultatet e synuara të propozimit? (jo më shumë se 7 rreshta)*Objektivat që synohen të arrihen nëpërmjet miratimit të kësaj politike janë: Rritja e sigurisë në rrjetet dhe sistemet e informacionit në Republikën e Shqipërisë, veçanërisht në infrastrukturat kritike dhe të rëndësishme të informacionit, përmes ngritjes së kapaciteteve teknike dhe ligjore. Plotësimi i kuadrit ligjor nërpërmjet dispozitave që parashikojnë ngritjen e strukturave dhe mekanizmave të nevojshme për garantimin e sigurisë kibernetike në nivel kombëtar, si dhe procedurave të lidhura me to brenda vitit 2025. Garantimi i sigurisë kibernetike përmes rregullimi të certifikimit të sigurisë kibernetike në përputhje me skemat e certifikimit të Bashkimit Evropian.Forcimi i masave të sigurisë kibernetike si dhe mbikëqyrjes së zbatimit të tyre, duke forcuar edhe sanksionet administrative brenda vitit 2025. Rritja e bashkëpunimit kombëtar dhe ndërkombëtar për forcimin e sigurisë kibernetike në vend dhe përmbushjen e detyrimeve ndërkombëtare në këtë fushë. Përafrimi i legjislacionit shqiptar në fushën e sigurisë kibernetike me acquis e BE-së. |
| **OPSIONET E POLITIKAVE***Cilat janë opsionet kryesore të politikave? Duhet të bëni krahasimin e avantazheve/përfitimeve kryesore dhe të dizavantazheve/kostove të opsioneve të mundshme. (jo më shumë se 7 rreshta)*Opsionet e mëposhtme janë vlerësuar në funksion të arritjes së politikave : **Opsioni 0** – Ruajtja e status quo-së pa ndërhyrje në kuadrin ligjor ekzistues, Ligji nr. 2/2017 “Për Sigurinë Kibernetike”. **Opsioni 1** – Amendimi i ligjit nr.2/2017 “Për Sigurinë Kibernetike”.**Opsioni 2** – Miratimi i një ligji të ri për sigurinë kibernetike.**Opsioni 0**: Nënkupton mosndërmarrjen e ndonjë politike duke vijuar me funksionimin sipas legjislacionit aktual. Ky opsion nuk kërkon kosto shtesë, por nga ana tjetër nuk ofron asnjë avantazh krahasuar me gjendjen ekzistuese të sigurisë kibernetike, mekanizmave dhe strukturave në këtë fushë si dhe procedurave përkatëse, në Republikën Shqipërisë. Ky opsion nuk ka kosto financiare shtesë dhe nuk kërkon burime njerëzore përveç fazës së monitorimit, por nga ana tjetër, nuk jep zgjidhje për problematikat e evidentuara të tilla si: trajtimi i krizës kibernetike, certifikimi i sigurisë kibernetike, kapacitetet e nevojshme teknike dhe ligjore për operatorët e infrastrukturave të informacionit etj.**Opsioni 1:** Amendimi i kuadrit ligjor ekzistues për fushën e sigurisë kibernetike. Kuadri ligjor ekzistues, ligji nr. 2/2017 “Për Sigurinë Kibernetike”, është i përafruar pjesërisht me Direktivën NIS1 të Bashkimit Evropian. Në kuadër të nevojës për përafrimin e pjesshëm të ligjit me Direktivën e BE-së NIS2, dhe bazuar në teknikën legjislative, duke qenë se ndryshimet që reflektohen në projektligj prekin më shumë se 50% të përmbajtjes së ligjit aktual, është e pamundur ndërmarrja e një nisme të tillë rregullatore. Gjithashtu, ky opsion ka kosto (kohë, burime njerëzore, financiare etj).**Opsioni 2:** Hartimi i një ligji të ri, në përputhje pjesërisht me Direktivën ( BE) nr. 2022/2555.Duke qenë se kuadri ligjor ekzistues që rregullon fushën e sigurisë kibernetike në Republikën e Shqipërisë është vetëm pjesërisht i përafruar me Direktivën NIS1 të BE-së, si dhe marrë në konsideratë faktin që Direktiva NIS 2 është miratuar dhe rrjedhimisht duhet transpozuar gradualisht në legjilacionin kombëtar, shihet e arsyeshme hartimi i një ligji të ri, duke përfshirë të gjithë elementët që aktualisht mungojnë në legjislacionin ekzistues. Ky opsion do të garantonte bazën e duhur ligjore për garantimin e sigurisë kibernetike për rrjetet dhe sistemet e informacionit në nivel kombëtar, duke krijuar mekanizmat e nevojshëm dhe vendosur rregulla të qarta për të gjitha palët e përfshira. Gjithashtu hartimi i një ligji të ri ka kosto të konsiderueshme, krahasuar me opsionet e tjera të marra në konsideratë.  |
| **ANALIZA E NDIKIMEVE***Cilat janë ndikimet e opsionit të preferuar? Kjo duhet të përshkruajë ndikimet në mënyrë sasiore (monetare) dhe cilësore (narrative) mbi buxhetin dhe grupet e tjera të prekura. (jo më shumë se 10 rreshta)*Ndikimet e drejtpërdrejta të opsionit të preferuar (**Opsioni 2)**:* Plotësimi i kuadrit ligjor në përputhje me linjën e BE-së duke futur elementët e rinj të cilët do të kompletojnë kornizën ligjore në fushën e sigurisë kibernetike.
* Rritja e sigurisë në rrjetet dhe sistemet e informacionit në Republikën e Shqipërisë, veçanërisht në infrastrukturat kritike dhe të rëndësishme të informacionit, përmes mekanizmave të rinj të parashikuara në dispozitat e projektligjit.
* Përcaktimi i strukturave përgjegjëse për sigurinë kibernetike, kompetencave dhe detyrave përkatëse lidhur me trajtimin dhe menaxhimin e incidenteve kibernetike.
* Forcimi i masave të sigurisë (teknike, organizative dhe operacionale) si dhe e mbikëqyrjes së zbatimit të tyre.
* Forcimi i bashkëpunimit në nivel kombëtar dhe ndërkombëtar.

Lidhur me ndikimet monetare: * Sjell të ardhura në buxhetin e shtetit të cilat burojnë nga tarifat e rritura të sanksioneve administrative. Si një përfitim jo i drejtpërdrejtë vlerësohet të jetë gjithashtu edhe përmirësimi i sigurisë.
* Nga ana tjetër, për ngritjen dhe funksionimin e strukturave të përcaktuara në dispozitat e projekt-ligjit si dhe përmbushjen e kompetencave dhe përgjegjësive të zgjeruara të strukturave ekzistuese, nevojiten kapacitete teknike dhe njerëzore të shtuara, që kërkojnë gjithashtu dhe investime të shtuara, duke pasur kështu një impakt negativ në buxhetin e shtetit.

Vlerësohet se kostoja është më e lartë se përfitimet për buxhetin e shtetit në terma afatshkurtër, rrjedhimisht ndikimi në buxhet do jetë negativ. Ndërsa, duke konsideruar edhe ndikimet jo të drejtpërdrejta, në terma afatgjatë, vlerësohet se investimet e kryera do të sillnin përfitime që do të ishin më të larta se kostot që mund të rrjedhin nga dobësitë e sigurisë kibernetike.  |
| **ARSYETIMI I OPSIONIT TË PREFERUAR** *Shpjegoni arsyet për zgjedhjen e opsionit të preferuar. Ju lutemi jepni nëse është e mundur koston dhe përfitimin me vlerë të përcaktuar monetare. (jo më shumë se 7 rreshta)* Opsioni i preferuar është zgjedhur **Opsioni 2,** pra miratimi i një ligji të ri “Për Sigurinë Kibernetike”, pasi:* Transpozimi i plotë i Direktivës NIS1 si dhe përfshirja e disa elementeve të Direktivës NIS2, do të kompletojë kornizën aktuale ligjore, duke përmbushur objektivin e përafrimit të legjislacionit vendas me atë të BE-së në kuadër të Planit Kombëtar të Integrimit Evropian të Republikës së Shqipërisë (2023-2025).
* Plotëson kuadrin ligjor duke përfshirë dispozita në lidhje me përcaktimin e subjekteve përgjegjëse për sigurinë kibernetike, ngritjen e strukturave dhe mekanizmave të nevojshme për garantimin e sigurisë kibernetike në nivel kombëtar, si dhe procedurave të lidhura me to, certifikimin e sigurisë kibernetike, mënyrën e raportimit dhe trajtimit të incidenteve, dhe trajtimin e krizës kibernetike.
* Rrit kërkesat dhe masat e sigurisë në infratsrukturat kritike dhe të rëndësishme të informacionit, si dhe forcon mbikëqyrjen e zbatimit të tyre.
* Rrit bashkëpunimin kombëtar dhe ndërkombëtar me qëllim forcimin e sigurisë kibernetike kombëtare.
* Ka impakt financiar në buxhetin e shtetit duke i sjellë atij të ardhura të cilat burojnë nga tarifat e rritura të sanksioneve administrative si dhe në terma afatgjatë sjell përfitime jo të drejtpërdrejta (si p.sh. përmirësimi i sigurisë kibernetike në nivel kombëtar, etj), ndonëse për momentin kostoja në buxhetin e shtetit parashikohet të jetë e lartë. Ka impakt financiar në Buxhetin e Shtetit pasi ky projektligj parashikon ngritjen e Qendrës Kombëtare të Sigurisë Kibernetike (SOC) si dhe trajnime të vazhdueshme të stafit të Autoritetit me qëllim ngritjen e kapaciteteve në këtë fushë.

Gjithashtu ky projektligj sjell efekte financiare për operatorët administrues lidhur me investimet që duhet të bëjnë në implementimin e masave të sigurisë për mbrojtjen e sistemeve dhe rrjeteve të tyre të informacionit nga rreziqet apo kërcënimet e mundshme kibernetike. Gjithsesi një parashikim i tillë nuk mund të shprehet në vlerë monetare pasi duhet të bëhet nga vetë infrastrukturat (investime në kapital, pajisje, burime njerëzore). Lidhur me analizën financiare për koston e opsionit të preferuar mbi buxhetin e shtetit, analiza është bërë në pjesën e dytë të RIA-së “*Vlerësimi i opsioneve/analizimi i ndikimeve.”* **Kostoja e përllogaritur në total e opsionit të preferuar mbi buxhetin e shtetit gjatë periudhës 3-vjeçare menjëherë pas miratimit të ligjit (kostoja në total në lek, çmimet aktuale, në terma nominalë):**

|  |  |
| --- | --- |
| **Viti** **1** | **Viti 2+Viti 3** |
| 2,000,000,000 lekë  | 5700076020 lekë |

\*Referuar përllogaritjes së bërë në Pjesën 2, “Vlerësimi i opsioneve/analizimi i ndikimeve”, tabela në fq 18.  |
| **KONSULTIMI***Jepni një përmbledhje të çdo konsultimi të kryer (me kë dhe si jeni konsultuar? (jo më shumë se 5 rreshta)*Projektligji është hartuar nga Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike si dhe është bashkëpunuar me Agjencinë Kombëtare të Shoqërisë së Informacionit. Gjithashtu janë zhvilluar takime dypalëshe të grupit të punës me Agjencinë Kombëtare të Shoqërisë së Informacionit, ku janë reflektuar në projektligj konkluzionet e arritura në lidhje me temat e diskutuara.Në datat 20 - 22 korrik u zhvillua një workshop me ekspertët e TAIEX për shpjegimin e Direktivës 2016/1148 (NIS Directive). Ekspertët u njohën edhe me draft ligjin e përgatitur nga ana e Autoritetit lidhur me qasjen ndaj Direktivës NIS 1 ku u shprehën se Drafti i ligjit “Për sigurinë kibernetike” përmban të giitha parashikimet e nevojshme për transpozimin e direktivës dhe se nevojiten vetëm disa detaje të vogla për t’u përfshirë lidhur me infrastrukturat e informacionit, duke dhënë kështu rekomandimet e tyre.  **Rekomandimet e dhëna i referoheshin mbrojtjes së infrastrukturave kritike të informacionit, përkatësisht:** 1. Për zhvillimin e mëtejshëm të kësaj fushe shihet e nevojshme njohja dhe shkëmbimi i njohurive dhe praktikave më të mira midis Republikës së Shqipërisë dhe autortiteteve të Bashkimit Evropian, të vendeve anëtare dhe vendeve të rajonit.
2. Procesi i përvetësimit të njohurive është një aktivitet afatgjatë dhe për këtë është e nevojshme të zbulohet se cilat njohuri dhe fusha kyçe duhet të përvetësohen, në mënyrë që ndërtimi i një sistemi të fuqishëm të mbrojtjes së infrastrukturës kritike të informacionit të jetë një aktivitet i planifikuar. Prandaj, është i nevojshëm zgjerimi i bashkëpunimit me komunitetin akademik, i cili mund të ofrojë njohuri dhe qasje që ndonjëherë mungojnë në këtë fazë për institucionet dhe individët.
3. Pjesëmarrja aktive e të gjitha ministrive që janë kompetente për politikat dhe planet sektoriale.

d) Konkretisht lidhur me këtë proces por edhe ndërtimin e sistemit, është e nevojshme të ketë dialog dhe bashkëpunim sa më të gjerë të mundshëm me të gjithë aktorët përkatës brenda çdo sektori. Kjo duhet të përfshijë ministritë, agjencitë rregullatore, operatorët e infrastrukturës së informacionit kritik, organizatat profesionale dhe deri te shërbimet e inspektimit.Këto rekomandime u shqyrtuan dhe u përfshin në projektligj, përkatësisht parashikimet lidhur me bashkëpunimin ( kombëtar dhe ndërkombëtar), infrastrukturat e informacionit ( masat e sigurisë, mbikëqyrja). Në datat 14-15 Dhjetor 2022 stafi i Autoritetit mori pjesë edhe në një trajnim të zhvilluar nga eGA lidhur me “Implementation of EU Cybersecurity Law”, trajnim në të cilin u shpjegua rreth Direktivës NIS 1 dhe NIS 2 duke bërë të mundur analizimin e elementëve të përfshirë në draft ligj si dhe reflektimin e rekomandimeve të dhëna lidhur me të dy Direktivat. Në këtë trajnim u sqaruan të dy direktivat duke përfshirë pika kryesore lidhur me autortietit mbikëqyrëse kompetente, CSIRT, infrastrukturat e informacionit, raportimi dhe reagimi ndaj incidenteve kibernetike. Gjithashtu në fokus ishin edhe skemat e certifikimit të sigurisë kibernetike, risi e Direktivës NIS 2, e përfshirë edhe në projektligj. Shpjegimet u shoqëruan edhe me shembuj të modeleve të vendeve të Bashkimit Europian. Nga trajnimi u dha një pasqyrë më e qatë e Direktivës NIS 2, të cilat u morën për bazë dhe u përfshin në projektligj përkatësisht elementët lidhur me infrastrukturat e informacionit, gjendjen e krizës kibernetike, skemat e certifikimit të sigurisë kibernetike.Në zbatim të ligjit nr.146/2014, “Për Njoftimin dhe Konsultimin Publik” projektligji “Për sigurinë kibernetike” u publikua në portalin e Regjistrit Elektronik për Njoftimet dhe Konsultimet Publike (RENJKP), nga data 26.04.2023 deri në datën 24.05.2023 (20 ditë pune). Në njoftimin e publikuar në regjistrin e konsultimeve publike u ftuan palët e interesuara për të marrë pjesë në takimet konsultative që do të zhvilloheshin nga Autoriteti në datat 9, 10 dhe 11 Maj. Gjatë kësaj periudhe Autoriteti në datat 9, 10 dhe 11 Maj zhvilloi takime konsultative me grupet e interesit. Paralelisht Autoriteti njoftoi me shkresë dhe e-mail infrastrukturat kritike dhe të rëndësishme të informacionit, për pjesëmarrjen e tyre. **Në datën 9 Maj** u zhvilluan takime konsultative me grupin e I, ku u përfshi sektori bankar, financiar (u dërgua shkresë Bankës së Shqipërisë, Shoqatës Shqiptare të Bankave, Shoqatës Mikrofinanciare Shqiptare, MFE, AMF, si dhe u njoftuan me e-mail të gjitha pikat e tyre të kontaktit).**Në datën 10 Maj**  u zhvilluan takime konsultative me grupin e II, ku u përfshi : Presidenca, Kuvendi, AKSHI, SHISH, AKSIK, ILDKPKI, PSH.**Në datën 11 Maj** u zhvilluan takime konsultative me grupin e III , ku u përfshi sektori i transportit, shëndetësor, furnizimit me ujë, energjia, AKEP.Në këto takime morën pjesë të gjitha infrastrukturat e informacionit si edhe subjekte të tjera të interesuara të cilët shfaqën interesin e tyre për pjesëmarrje nga njoftimi në regjistrin e konsultimeve publike. Në këto takime u paraqitën risitë e projektligjit si dhe u diskutua lidhur me komentet dhe sugjerimet e pjesëmarrësve lidhur me projektligjin.Në vijim të këtyre takimeve u dërguan komentet dhe sugjerimet me shkrim nga infrastrukturat (bankat). Përmes Regjistrit Elektronik për Njoftimet dhe Konsultimet Publike (RENJKP) ka pasur interesim të publikut për nismën ligjore gjë e cila tregohet nga numri i leximeve, ku në total ka pasur ***1031*** lexime dhe ***1*** koment nga një qytetar referuar vënies në dispozicion të tabelës së përputhshmërisë. Nëpërmjet sistemit e-akte si dhe me shkrim institucionet të cilat kanë përcjellë komente dhe sugjerime janë : Ministri i Shtetit dhe Kryenegociatori , Departamenti i Administratës Publike, Ministria e Drejtësisë, Agjencia Kombëtare e Shoqërisë së Informacionit, Ministria e Infrastrukturës dhe Energjisë, Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, Autoriteti Kombëtar i Sigurisë së Informacionit të Klasiffikuar, Ambasada Amerikane, Shoqata Shqiptare e Bankave, Banka e Shqipërisë, Ministria e Brendshme.Kryesisht komentet ishin të një natyre teknike, dhe i referoheshin elementëve teknikë në përmbajtje të dispozitave (shpjegime kryesisht nga ana e bankave) si dhe komente apo sygjerime lidhur me nene specifike referuar CSIRT-eve, CERT, gjendjes së krizës kibernetike, bashkëpunimit, raportimit të incidentit kibernetik (afati/mënyra e raportimit), skemës së certifikimit të sigurisë kibernetike, kundravajteve administrative, masës së gjobave. Ambasada Amerikane në komentet e dhëna kishte fokus bashkëpunimin me Policinë e Shtetit dhe Prokurorinë. Shpjegimet përkatëse për secilin koment janë dhënë në Raportin Individual të Konsultimit Publik për projektligjin.Marrë në konsideratë ndryshime e sjella nga Direktiva NIS 2 si dhe bazuar në rekomandimin e takimit të Nenkomitetit “Inovacioni, Shoqeria e informacionit dhe politikat sociale” të datës 2 shkurt 2023, i cili rekomandon: *Përafrim të plotë me Direktivën (BE) nr.2022/2555 (NIS 2)* të projektligjit “Për sigurinë kibernetike”, Autoriteti ka punuar për zbatimin e rekomandimit duke përafruar projektligjin me Direktivën NIS 2 . Drafti u rishikua dhe u ripunua si dhe me 30.08.2023 u dërgua në Kryeministri për vijimin me procedurat e mëtejshme. Drafti u hodh në sistemin e akte ku janë përcjellë mendimet e Ministria e Drejtësisë, Departamenti i Administratës Publike, Ministria e Financës dhe Ekonomisë, Ministria e Brendshme, Ministria e Arsimit dhe Sportit, Agjencia Kombëtare e Shoqërisë së Informacionit, Ministria e Infrastrukturës dhe Energjisë, Ministri Shtetit dhe Kryenegociatori, Autoriteti Kombëtar i Sigurisë së Informacionit të Klasifikuar, Kryesisht mendimet e sjella konstistonin në shprehjen e dakordësisë si dhe sugjerime lidhur me terminologjinë e përdorur, plotësimi i disa dispozitave lidhur me element konkret teknikë si dhe dhënia e shpjegimeve në lidhje me efektet fiannciare të projektligjit. Komentet janë marrë në konsideratë dhe janë reflektuar në draftin aktual. |
| **ZBATIMI DHE MONITORIMI***Si do të organizohen zbatimi dhe monitorimi?(jo më shumë se 5 rreshta)*Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (me hyrjen në fuqi të këtij ligji, emri i institucionit do ndryshojë nga AKCESK në Autoriteti Kombëtar për Sigurinë Kibernetike), është institucioni përgjegjës për rregullimin dhe mbikëqyrjen e fushës së sigurisë kibernetike në Republikën e Shqipërisë. Autoriteti do të hartojë aktet përkatëse nënligjore dhe do të mbikëqyrë subjektet në përputhje me kërkesat e këtij projektligji. Subjektet përgjegjëse për zbatim janë Autoritet përgjegjës për Sigurinë Kibernetike si dhe subjektet e tjera përgjegjëse për sigurinë kibernetike sipas përcaktimeve të bëra në këtë projektligj[[1]](#footnote-1):  Subjektet e tjera përgjegjëse për sigurinë kibernetike janë: Ministria përgjegjëse për sektorin e energjisë dhe transportit,telekomunikacionit dhe shërbimit postar, Ministria përgjegjëse për rendin dhe sigurinë publike, Ministria përgjegjëse për sektorin e ekonomisë dhe financës, Ministria përgjegjëse për sektorin e kujdesit shëndetësor, Ministria përgjegjëse për mjedisin, turizmin, mbrojtjen e territorit dhe funksione të tjera të lidhura me të, Ministria përgjegjëse për bujqësinë dhe funksione të tjera të lidhura me të, Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI), institucionet e tjera përgjegjëse për ruajtjen dhe përpunimin e të dhënave qeveritare, çdo institucion tjetër publik i pavarur që administron infrastruktura të informacionit në kuptim të këtij ligji.Subjektet përgjegjëse sektoriale të sigurisë së rrjeteve dhe sistemeve të informacionit: Subjektet që ofrojnë shërbime në sektorët e energjisë, përfshirë sektorët e energjisë elektrike, gazit naftës dhe energjisë bërthamore, Subjektet që ofrojnë shërbime në sektorët e transportit ajror, detar, hekurudhor, rrugor dhe postar, telekomunikacioni, Subjektet që ofrojnë shërbime në sektorët e ekonomisë, financës, infrastrukturës së tregut financiar, sektorin bankar, si dhe sistemet mikrofinanciare, Subjektet që ofrojnë shërbime në tregun e siguracioneve, shoqëritë e sigurimit, Policia e shtetit si subjekt me mision ruajtjen e rendit e të sigurisë publike, Subjektet që ofrojnë shërbime në sektorët e kujdesit e ndihmës shëndetësore të të autorizuar dhe të akredituar nga autoritetet përgjegjëse, Subjektet që ofrojnë shërbime në sektorët e mjedisit dhe mbrojtjes së territorit dhe autoritetet territoriale përgjegjëse për furnizimin dhe shpërndarjen e ujit të pijshëm, Subjektet që ofrojnë shërbime në sektorët e infrastrukturës digjitale, telekomunikacionit, si dhe shërbimet digjitale, Subjektet që ofrojnë shërbime në sektorin akademik. |

|  |
| --- |
| **PJESA 2: BAZA KRYESORE E ANALIZËS DHE E PROVAVE**  |

# Historik

*Jepni kontekstin e politikës.*

Rrjetet dhe sistemet e informacionit luajnë një rol të rëndësishëm në shoqërinë shqiptare. Siguria dhe besueshmëria e tyre është po aq e rëndësishme sa edhe vetë ekzistenca e këtyre rrjeteve dhe sistemeve. Shkalla, shpeshtësia dhe ndikimi i incidenteve të sigurisë janë në rritje dhe përfaqësojnë një shqetësim dhe kërcënim serioz për funksionimin e rrjeteve dhe sistemeve të informacionit, gjithashtu edhe të vetë funksionimit të shtetit. Sisteme të tilla mund të bëhen gjithashtu një objektiv për veprime që synojnë të dëmtojnë ose prishin funksionimin e sistemeve.

Sulmet kibernetike të vitit të shkuar që shenjëstruan institucionet shqiptare si dhe sofistikimi i tyre, kërkon kapacitete teknike dhe njerëzore të shtuara, struktura të posaçme për t’i parandaluar, menaxhuar dhe zgjidhur ato, nisma të reja si dhe masa të shtuara, me qëllim mbrojtjen e sigurisë kombëtare nga kërcënimet e këtij lloji. Direktiva (BE) 2016/1148 të Parlamentit Evropian dhe Këshillit e datës 6 korrik 2016 “Në lidhje me masat për një nivel të lartë të përbashkët të sigurisë së rrjeteve dhe sistemeve të informacionit në të gjithë Bashkimin Evropian” është pjesa e parë e legjislacionit të sigurisë kibernetike në Bashkimin Evropian[[2]](#footnote-2).

Në nenin 1 të saj përcaktohet se kjo Direktivë ka si qëllim përcaktimin e masave për garantimin e një niveli të lartë të sigurisë kibernetike në të gjithë Bashkimin Evropian si dhe përmirësimin e funkionimit të tregut të brendshëm. Direktiva NIS synon të vendosë gjerësisht standarde dhe praktika të përbashkëta të sigurisë në të gjithë BE-në. Direktiva NIS u miratua në vitin 2016 dhe më pas, duke qenë një direktivë e BE-së, çdo shtet anëtar i BE-së ka filluar të miratojë legjislacionin kombëtar, i cili ndjek ose ‘transpozon’ direktivën.

Ligji nr.2 datë 26.01.2017 “Për Sigurinë Kibernetike” është pjesërisht i përafruar me Direktivën (BE) 2016/1148 të Parlamentit Europian dhe të Këshillit, datë 6 korrik 2016, “Mbi masat për një nivel të përbashkët të lartë të sigurisë së rrjeteve dhe sistemeve të informacionit në Bashkimin Europian”.[[3]](#footnote-3)

Kuadri ligjor aktual ka si qëllim arritjen e një niveli të lartë të sigurisë kibernetike, duke përcaktuar masat e sigurisë, të drejtat, detyrimet, si dhe bashkëpunimin e ndërsjellët ndërmjet subjekteve që operojnë në fushën e sigurisë kibernetike.

Pra kuadri ligjor aktual përcakton Autoritetin si institucioni përgjegjës për sigurinë kiberneitke në vend, kompetencat e këtij të fundit në fushën e sigurisë kibernetike, Ekipin Përgjegjës ndaj Incidenteve të Sigurisë Kibernetike, parashikime lidhur me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, masat e sigurisë, raportimin e incidenteve, administrimin e sigurisë kibernetike etj.

Neni 70 i Marrëveshjes së Stabilizim Asocimit (MSA) përcakton angazhimin e Shqipërisë për përafrimin e legjislacionit ekzistues me acquis e BE-së. Plani Kombëtar për Integrimin Evropian ka për qëllim të koordinojë këtë proces përafrimi duke synuar njëkohësisht plotësimin e detyrimeve në kuadër të MSA dhe detyrimet që lindin në kuadër të procesit të anëtarësimit në Bashkimin Evropian.

Në Planin Kombëtar për Integrimin Evriopian (PKIE) 2023-2025 është parashikuar transpozimi i plotë i Direktivës (BE) 2016/1148 të Parlamentit Europian dhe të Këshillit, datë 6 korrik 2016, “Mbi masat për një nivel të përbashkët të lartë të sigurisë së rrjeteve dhe sistemeve të informacionit në Bashkimin Europian”, fushë e përgjegjësisë së Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetik.

Gjithashtu me hyrjen në fuqi të Direktivës (BE) nr.2022/2555 të Parlamentit dhe Këshillit Evropian, datë 14 dhjetor 2022 “Mbi masat për një nivel të lartë të përbashkët të sigurisë kibernetike në të gjithë Bashkimin Evropian”[[4]](#footnote-4), duke ndryshuar Rregulloren (BE) nr.910/2014 dhe Direktivën (BE) nr. 2018/1972, dhe duke shfuqizuar Direktivën (BE) nr. 2016/1148 me efekt prej 18 tetorit 2024 (NIS 2)”[[5]](#footnote-5), si dhe bazuar në rekomandimin e takimit të Nenkomitetit “Inovacioni, Shoqeria e informacionit dhe politikat sociale” të datës 2 shkurt 2023, i cili rekomandon: *Përafrim të plotë me Direktivën (BE) nr.2022/2555 (NIS 2)* të projektligjit “Për sigurinë kibernetike”, u pa e nevojshme përfshirja e disa elementëve të kësaj Direktive, me qëllim përditësimin dhe plotësimin e legjislacionit në fushën e sigurisë kibernetike duke ndjekur qasjen e Bashkimit Evropian. ( PKIE 2023-2025) .

NIS 2 ka një fushë veprimi më të gjërë duke e përfshirë Direktivën NIS 1 si dhe duke bërë edhe specifikime të tjera.

# Problemi në shqyrtim

1. *Përshkruani natyrën e problemit.*
2. *Identifikoni shkaqet e problemit.*
3. *Përshkruani shtrirjen e problemit.*
4. *Identifikoni grupet e prekura nga ky problem - qeveria / biznesi / shoqëria civile / qytetarët.*
5. *Vlerësoni nëse problemi mund të trajtohet ose jo përmes një ndryshimi të politikave.*

Problemi lidhet me nevojën për forcimin e nivelit të sigurisë kibernetike në vend ku korniza ligjore luan një rol të rëndësishëm për të krijuar hapësirat e ndërmarrjes së iniciativave dhe masave të nevojshme në nivel kombëtar, të cilat duhet të jenë të parashikuara dhe në përputhje me legjilacionin në fuqi. Në legjislacionin aktual identifikohen disa problematika të cilat pengojnë realizimin e objektivave për garantimin e një niveli të lartë të sigurisë kibernetike dhe ndërhyrjen e qeverisë për zbatimin e nismave të reja dhe forcimin e masave të sigurisë.

Po ashtu, në kuadër të angazhimeve të shtetit shqiptar për integrimin e Shqipërisë në Bashkimin Evropian, ekziston nevoja e përmirësimit të kuadrit ligjor në vend duke e përafruar me acquis të BE, në përputhje dhe me Planin Kombëtar të Integrimit Evropian 2023-2025. Rrjedhimisht, lind nevoja për përmirësimin e legjislacionit për arritjen e objektivave strategjike të qeverisë shqiptare për forcimin e sigurisë kibernetike në vend dhe përshpejtimin e procesit të integrimit evropian.

**Disa nga shkaqet e problemit të konstatuar dhe mangësitë e evidentuara janë si më poshtë vijon:**

* Mungesa e parashikimeve të qarta ligjore lidhur me subjektet përgjegjëse të sigurisë kibernetike dhe detyrat përkatëse të tyre: CSIRT Kombëtar (Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kibernetike, pranë Autoritetit), CSIRT Sektorial (Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kibernetike, për sektorin përkatës) dhe CSIRT pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit (Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kibernetike pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit).
* Mungesa e parashikimeve në kuadrin ligjor për ngritjen e një strukture që bën monitorimin e sigurisë kibernetike në nivel kombëtar (Qendra Operacionale e Sigurisë Kibernetike ( SOC).
* Mungesa e parashikimeve ligjore lidhur me trajtimin e gjendjes së situatave emergjente, krizës kibernetike si dhe strukturave përkatëse për menaxhimin e tyre (CERT- Ekipi i Përgjigjes ndaj Emergjencave të Sigurisë Kibernetike).

• Mungesa e dispozitave lidhur me certifikimin e sigurisë kibernetike dhe procedurat përkatëse.

* Mungesa e parashikimeve të qarta ligjore lidhur me administrimin e sigurisë kibernetike (masat e sigurisë, masat për menaxhimin e riskut, raportimin e incidenteve kibernetike).

Për sa i përket grupeve të prekura nga ky problem, vlerësohet se janë qeveria, subjektet e tjera përgjegjëse për sigurinë kibernetike, përfshirë operatorët e infrastrukturave të informacionit, si dhe bizneset që operojnë në fushën e teknologjisë së informacionit dhe komunikimit, administrata publike, dhe qytetarët, pasi shërbimet që ofrojnë ose marrin këto grupe duhet të jenë të sigurta dhe të garantojnë privatësinë sipas parimeve të sigurisë kibernetike të.

A**rsyeja e ndërhyrjes**

1. *Shpjegoni pse qeveria e sheh të nevojshme të ndërhyjë.*
2. *Shpjegoni se çfarë shpreson të trajtojë qeveria nëpërmjet kësaj ndërhyrjeje.*
3. *Shpjegoni se si i mbështet kjo ndërhyrje objektivat e nivelit të lartë të qeverisë.*
4. *Rendisni punën ekzistuese që është realizuar tashmë.*

Siguria kibernetike ka rol thelbësor në sigurinë kombëtare pasi cenimi i sigurisë së rrjeteve dhe sistemeve të informacionit në Republikën e Shqipërise do të dëmtonte interesat kombëtare dhe sigurinë e vendit në tërësi. Probematikat e evidentuara kërkojnë një legjislacion të ri dhe të përmirësuar në përputhje me acquis e BE-së për të mundësuar garantimin dhe forcimin e sigurisë kibernetike në vend. Ndërhyrja e qeverisë është e nevojshme pasi do t’i jepte zgjidhje problematikave të përmendura më sipër që janë identifikuar gjatë zbatimit të legjislacionit ekzistues.

Sulmet kibernetike të vitit të shkuar që shenjëstruan institucionet shqiptare kanë rritur nevojën për përmirësimin e sigurisë kibernetike përmes shtimit të kapaciteteve teknike dhe ligjore të nevojshme, duke përfshirë krijimin e strukturave dhe mekanizmave të nevojshme dhe përcaktimin e procedurave dhe detyrave respektive, ndërmarrjen e nismave dhe masave të shtuara, si dhe rritjen e bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike. Në këtë kuadër shihet e nevojshme rritja e nivelit të sigurisë kibernetike në vend duke krijuar strukturat e duhura për mbrojtjen efektive ndaj sulmeve të mundshme kibernetike.

Kapacitetet e deritanishme nuk janë të mjaftueshme për të garantuar një nivel të lartë sigurie në rrjetet dhe sistemet e informacionit. Përgatitja e përgjigjeve ndaj sulmeve apo incidenteve kibernetike nuk mjafton në nivelin që ato paraqiten, dhe kjo çon në domosdoshmërinë e ngritjes së kapaciteteve të reja teknike dhe ligjore.

Për një përgjigje sa më efektive ndaj sfidave të sigurisë së rrjeteve dhe sistemeve të informacionit është e nevojshme një qasje gjithëpërfshirëse në nivel shtetëror dhe më gjerë në nivel ndërkombëtar, që do të përfshijë krijimin e kapaciteteve minimale por njëkohësisht të larta dhe të mjaftueshme me qëllim planifikimin, shkëmbimin e informacionit, bashkëpunimin dhe detyrimet e përbashkëta të sigurisë për operatorët e infrastrukturave kritike të informacionit dhe operatorët e infrastrukturave të rëndësishme të informacionit.

Gjithsesi pavarësisht përcaktimeve ligjore aktuale marrë në konsideratë rëndësinë që paraqet siguria kibernetike si dhe qenia konform e parashikimeve ligjore me acquis e Bashkimit Evropian, shihet si e nevojshme rishikimi dhe përditësimi i kuadrit ligjor aktual referuar kompetencave të Autoritetit, subjekteve përgjegjëse të sigurisë kibernetike, përcaktimit të strukturave dhe mekanizmave të duhura, operatorëve të infrastrukturave të nformacionit, masave të sigurisë, aktivitetit mbikëqyrës, forcimit të bashkëpunimit në nivel kombëtar dhe ndërkombëtar.

Përmes kësaj ndërhyrje, qeveria do të plotësonte kornizën ligjore të nevojshme për të marrë masat e duhura për adresimin e problematikave të evidentuara. Ndërhyrja e qeverisë do të ndikonte në rritjen e sigurisë për rrjetet dhe sistemet e informacionit në vend, veçanërisht infrastrukturat kritike dhe të rëndësishme të informacionit, duke siguruar strukturat dhe procedurat e nevojshme për monitorimin, parandalimin, menaxhimin dhe zgjidhjen e incidenteve kibernetike, si dhe mundësuar një skemë kombëtare për certifikimin e sigurisë kibernetike, për certifikimin e produkteve dhe proceseve të veçanta TIK.

Siguria kibernetike dhe integrimi evropian janë prioritete të qeverisë shqiptare, përmendim këtu Programin Qeverisës 2021-2025[[6]](#footnote-6) si dhe Strategjinë Kombëtare për Sigurinë Kibernetike dhe të planit të veprimit 2020–2025[[7]](#footnote-7). Kjo ndërhyrje e qeverisë është në kuadër të përafrimit të legjislacionit shqiptar me atë të Bashkimit Evropian (PKIE 2023-2025). Dispozitat e këtij projektligji krijojnë gjithashtu hapësirat e nevojshme ligjore për të vepruar në kuadër të arritjes së qëllimeve dhe objektivave strategjike të qeverisë në fushën e sigurisë kibernetike si dhe kontribuojnë në zbatimin e Planit Kombëtar të Integrimit Evropian përmes transpozimit të acquis së BE-së.

Puna ekzistuese e realizuar:

Në datat 20 - 22 korrik u zhvillua një workshop me ekspertët e TAIEX për shpjegimin e Direktivës 2016/1148 (NIS Directive). Ekspertët u njohën edhe me nismën e marrë nga ana e Autoritetit lidhur me qasjen ndaj Direktivës NIS 1 ku u shprehën se :

1. AKCESK ka treguar një përkushtim të fortë në arritjen e një shkalle të lart pjekurie lidhur me kuadrin ligjor të sigurisë kibernetike në përputhje me legjislacionin e BE-së.
2. Ndërtimi dhe rregullimi i kuadrit normativ për mbrojtjen e infrastrukturës kritike të informacionit (hartimi dhe nxjerrja e ligjeve dhe akteve nënligjore) instituconi përgjegjës – Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) ka punuar me përkushtim deri më tani për të.

Sa i përket nevojës për kapacitete të shtuara në fushën e sigurisë kibernetike, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike ka realizuar trajnime me përfaqësues të institucioneve dhe operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit dhe ka mundësuar trajnime të avancuara për stafin e vetë Autoritetit.

Autoriteti bashkëpunon me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, monitoron infrastrukturat kritike si dhe menaxhon incidentet kibernetike në infrastrukturat kritike, duke ofruar gjithashtu mbështetje për rritje kapacitetesh përmes trajnimeve dhe stërvitjeve kibernetike, si dhe mbështetje metodike për operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit.

Në kuadër të bashkëpunimit për adresimin e sfidave dhe rritjes së nivelit të sigurisë kibernetike në vend, janë nënshkruar marrëveshje bashkëpunimi me subjekte publike dhe private në nivel kombëtar, si dhe marrëveshje me institucione publike dhe private ndërkombëtare të shteteve partnere më të cilat Shqipëria bashkëpunon.

Në kuadër të rritjes së bashkëpunimit ndërkombëtar, si dhe më qëllim shkëmbimin e informacionit për incidentet kibernetike, eksperiencës, ngritjes së kapaciteteve teknike dhe njerëzore, AKCESK ka iniciuar nënshkrimin e marrëveshjeve të bashkëpunimit me partnerë strategjik dhe kompani ndërkombëtare të fushës së sigurisë kibernetike me institucionet dhe kompanitë: MoU me Izraelin, Marrëveshje Bashkëpunimi me 4IG, MoU me Këshillin e Sigurisë Kibernetike të Emirateve të Bashkuara Arabe, Marrëveshje Bashkëpunimi Shoqata Shqiptare e Bankave (AAB), Marrëveshje Bashkëpunimi me CyBureau.

Marrëveshje bashkëpunimi me subjekte publike dhe private në nivel kombëtar:Marrëveshje Bashkëpunimi me Raiffeisen Bank, Marrëveshje Bashkëpunimi me Autoritetin e Mediave Audiovizive dhe Qendrën e Koordinimit Kundër Ekstremizmit të Dhunshëm, Marrëveshje Bashkëpunimi me Autoritetin e Mediave Audiovizive dhe Qendrën e Koordinimit Kundër Ekstremizmit të Dhunshëm, Memorandum Mirëkuptimi midis Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike dhe Akademisë së Studimeve Politike, Memorandum Bashkëpunimi me AKEP, Marrëveshje Bashkëpunimi me Autoritetin Rregullativ të Komunikimeve Elektronike dhe Postare/Njësia Nacionale për Sigurinë Kibernetike e Republikës së Kosovës, Marrëveshje Bashkëpunimi me Autoritetin Rregullativ të Komunikimeve Elektronike dhe Postare/Njësia Nacionale për Sigurinë Kibernetike e Republikës së Kosovës, Memorandum Mirëkuptimi me AKSHI ( Republika e Shqipërisë) dhe Agjencisë Kombëtare për Përgjigje ndaj incidenteve kibernetike Republika e Rumanisë, Marrëveshje Bashkëpunimi midis AKCESK , AKSHI dhe Agjencisë për Komunikimet Elektronike të Republikës së Maqedonisë, Qendrës Kombëtare për Përgjigje ndaj Incidenteve Kibernetike.

Janë ndërmarrë gjithashtu disa hapa paraprake (referuar financimit, rekrutimit të stafit, bashkëpunimit) për t’i paraprirë ngritjes së Qendrës operacionale Kombëtare të Sigurisë Kibernetike që do të kryejë monitorimin e sigurisë kibernetike në nivel kombëtar, punë e cila do të vijojnë më tej dhe do të finalizohet pas implementimit të kësaj nisme në kuadër të së cilës parashikohet i administrimi i saj si një kompetencë e Autoritetit Kombëtar për Sigurinë Kibernetike.

Për ngritjen e Qendrës Kombëtare Operacionale të Sigurisë Kibernetike, me të gjithë komponentët përbërës të saj, si ato teknike, infrastrukturore dhe burime njerëzore, që prej mesit të muajit tetor 2022 e në vazhdim, konkretisht janë hedhur hapat si më poshtë:

* Janë realizuar takime bilaterale me partneret strategjike si: Departamenti i Shtetit USA, Mbretëria e Emirateve të Bashkuara Arabe, Qeveria e Izraelit, për të ndërtuar urat e bashkëpunimit në terma të mbështetjes së Shqipërisë për forcimin e sigurisë kibernetike.
* Është analizuar situata e sigurisë kibernetike të infrastrukturave kritike, me qëllim projektimin e Qendrës Kombëtare Operacionale për Sigurinë Kibernetike, duke përfshire National & Sectorial SOC.
* Janë adresuar dhe dakordësuar nevojat dhe buxhetet përkatëse, të AKCESK, AKSHI, Policisë së Shtetit dhe SHISH me përfaqësuesit e Departamentit të Shtetit, në funksion të mbështetjes financiare të vënë në dispozicion nga këta të fundit në ndihmë të Shqipërisë.
* Janë hartuar dhe dakordësuar termat e bashkëpunimit të marrëveshjes së mirëkuptimit me UAE, për sigurimin e mbështetjes së tyre për ngritjen Qendrës Kombëtare Operacionale për Sigurinë Kibernetike.
* Është bashkërenduar puna me DAP dhe ka përfunduar draftimi i paketës së plotë për strukturën e re të AKCESK e cila do të fillojë të implementohet në fillim të shkurtit dhe do të jetë tërësisht në funksion në fillim të vitit 2024.
* Në janar 2023, ka filluar bashkërendimi i punës me AKSHI për hartimin e termave të referencës mbi dy sisteme/platforma, në funksion të Qendrës Operacionale, të cilat do të realizohen nëpërmjet buxhetit të shtetit të miratuar për vitin 2024, gjatë 6 mujorit të parë të vitit.
* Gjithashtu përgjatë periudhës korrik-shtator AKCESK ka ngritur një sërë laboratorësh si pjesë e Qendrës Kombëtare Operacionale të Sigurisë Kibernetike (SOC), me qëllim monitorimin aktiv dhe analizën e kërcënimeve kibernetike në funksion të mbrojtjes së infrastrukturave kritike dhe të rëndësishme të informacionit. Konkretisht janë në funksion laboratorët:
* forensic, nëpërmjet të cilës investigohet natyra e incidenteve kibernetike;
* analizës së programeve keqdashëse;
* analizës së vulnerabiliteteve, nëpërmjet identifikimit të dobësive dhe testimin e rezistencës/qëndrueshmërisë së infrastrukturave të informacionit;
* për ndarjen e informacionit (MISP).

# Objektivi i politikës

1. *Vendosni objektiva që korrespondojnë me problemin dhe shkaqet e tij.*
2. *Sigurohuni që objektivat e vendosur të korrespondojnë me ato të dhëna në përmbledhjen ekzekutive, por më të detajuara.*
3. *Sigurohuni që objektivat janë specifikë, të matshëm, të arritshëm, realë dhe në kohë.*

Nëpërmjet kësaj nisme, synohet përmbushja e objektivave të mëposhtme:

* Rritja e sigurisë në rrjetet dhe sistemet e informacionit në Republikën e Shqipërisë, veçanërisht në infrastrukturat kritike dhe të rëndësishme të informacionit, brenda 2 viteve nga hyrja ne fuqi e këtij projektligji.
* Garantimi i nje niveli të lartë të sigurisë kibernetike ne vend nëpërmjet plotësimit te kuadrit ligjor brenda vitit 2025.
* Garantimi sigurisë kibernetike përmes rregullimit të certifikimit të sigurisë kibernetike në përputhje me skemat e certifikimit të Bashkimit Evropian.
* Forcimi i masave të sigurisë kibernetike si dhe mbikëqyrjes së zbatimit të tyre, duke forcuar edhe sanksionet administrative brenda vitit 2025.
* Rritja e bashkëpunimit kombëtar dhe ndërkombëtar për forcimin e sigurisë kibernetike në vend dhe përmbushjen e detyrimeve ndërkombëtare në këtë fushë.
* Përafrimi i legjislacionit shqiptar në fushën e sigurisë kibernetike me acquis e BE-së.

# Përshkrimi i opsioneve të shqyrtuara

1. *Përshkruani opsionin e status quo-së.*
2. *Identifikoni dhe përshkruani të gjitha opsionet e politikave që keni marrë parasysh.*
3. *Shpjegoni se si janë identifikuar opsionet e politikës.*

Opsionet e mëposhtme janë vlerësuar në funksion të arritjes së politikave:

**Opsioni 0** – Ruajtja e status quo-së pa ndërhyrje në kuadrin ligjor ekzistues, Ligji Nr. 2/2017 “Për Sigurinë Kibernetike”.

**Opsioni 1** – Amendimi i kuadrit ligjor ekzistues Ligji nr.2/2017 “Për Sigurinë Kiernetike

**Opsioni 2** – Miratimi i një ligji të ri.

**Opsioni 0**: Nënkupton mosndërmarrjen e ndonjë politike duke vijuar me funksionimin sipas legjislacionit aktual. Ky opsion nuk kërkon kosto shtesë, por nga ana tjetër nuk ofron asnjë avantazh krahasuar me gjendjen ekzistuese të sigurisë kibernetike, mekanizmave dhe strukturave në këtë fushë si dhe procedurave përkatëse, në Republikën Shqipërisë. Ky opsion nuk ka kosto financiare shtesë dhe nuk kërkon burime njerëzore përveç fazës së monitorimit, por nga ana tjetër, nuk jep zgjidhje për problematikat e evidentuara të tilla si: trajtimi i krizës kibernetike, certifikimi i sigurisë kibernetike, kapacitetet e nevojshme teknike dhe ligjore për operatorët e infrastrukturave të informacionit, masat e sigurisë kibernetike etj.

**Opsioni 1:** Amendimi i kuadrit ligjor ekzistues për fushën e sigurisë kibernetike. Në kuadër të nevojës për përafrimin e plotë të ligjit me Direktivën NIS1 të BE-së dhe përfshirjen e elementeve nga Direktiva NIS2 e BE-së, dhe bazuar në teknikën legjislative, duke qenë se ndryshimet që reflektohen në projektligj prekin më shumë se 50% të përmbajtjes së ligjit aktual, është e pamundur ndërmarrja e një nisme të tillë rregullatore. Gjithashtu, ky opsion ka kosto (kohë, burime njerëzore, financiare etj).

**Opsioni 2:** Hartimi i një ligji të ri, në përputhje të plotë me Direktivën NIS1 dhe pjesësisht me NIS2.

Duke qenë se kuadri ligjor ekzistues që rregullon fushën e sigurisë kibernetike në Republikën e Shqipërisë është vetëm pjesërisht i përafruar me direktivën NIS1 të BE-së, dhe duke qenë se është miratuar edhe direktiva NIS2 dhe duhet transpozuar gradualisht në legjilacionin kombëtar, shihet e arsyeshme hartimi i një ligji të ri, duke përfshirë të gjithë elementët që aktualisht mungojnë në legjislacionin ekzistues. Ky opsion do të garantonte bazën e duhur ligjore për garantimin e sigurisë kibernetike për rrjetet dhe sistemet e informacionit në nivel kombëtar, duke krijuar mekanizmat e nevojshëm dhe vendosur rregulla të qarta për të gjithë palët e përfshira. Pavarësisht se hartimi i një ligji të ri shoqërohet me kosto më të larta në krahasim me opsionin 1, si dhe me kosto të konsiderueshme në krahasim me opsionin status quo, avantazhet që ky opsion paraqet i justifikojnë plotësisht këto kosto. Nëpërmjet këtij opsioni do të mundësohet arritja e objektivave të vendosur, zgjidhja e problemeve të evidentuara duke ruajtur njëkohësisht qartësinë e legjislacionit të zbatueshëm në këtë fushë.

# Vlerësimi i opsioneve/analizimi i ndikimeve

1. *Identifikoni grupet e prekura.*
2. *Identifikoni llojet e ndikimeve për secilin grup të prekur, bëni dallimin midis ndikimeve të drejtpërdrejta dhe jo të drejtpërdrejta.*
3. *Për ndikimet e drejtpërdrejta:*

* 1. *Përshkruani nga ana cilësore ndikimet e drejtpërdrejta mbi grupet e prekura.*
	2. *Analizoni nga ana sasiore ndikimet më të rëndësishme të drejtpërdrejta.*
	3. *Përcaktoni vlerën monetare të ndikimeve më të rëndësishme të drejtpërdrejta aty ku është e mundur (përdor tabelën në Aneksin 2/a të këtij dokumenti).*
	4. *Analizoni ndikimin mbi ndërmarrjet e vogla dhe të mesme (nëse ka).*
1. *Për ndikimet jo të drejtpërdrejta:*
	1. *Përshkruani nga ana cilësore ndikimet jo të drejtpërdrejta mbi grupet e prekura.*
	2. *Analizoni ndikimin mbi konkurrencën.*
2. *Diskutoni kufizimin e analizës:*
	1. *Jepni supozimet në të cilat janë bazuar parashikimet dhe risqet, të cilave ato u nënshtrohen.*
	2. *Tregoni se çfarë mund të pengojë realizimin e përfitimeve, të rrisë kostot ose të sjellë pasoja të papritura.*
3. *Përmblidhni vlerësimin e opsioneve:*
	1. *Paraqisni një pasqyrë përmbledhëse të të gjitha ndikimeve të opsioneve të analizuara.*
	2. *Shpjegoni se si ndikimet e të gjitha opsioneve të analizuara krahasohen me njëra-tjetrën.*
	3. *Paraqisni përllogaritjet më të mira të përgjithshme neto të ndikimit me vlerë monetare të përcaktuar për çdo opsion (përdor tabelën në Aneksin 2/b të këtij dokumenti).*

**Grupet e prekura**: Miratimi i një projektligji të ri për sigurinë kibernetike do të ketë një ndikim mbi qeverinë, subjektet e tjera përgjegjëse për sigurinë kibernetike sipas përcaktimeve të bëra në këtë projektligj, përfshirë operatorët e infrastrukturave të informacionit, si dhe bizneset që operojnë në fushën e teknologjisë së informacionit dhe komunikimit, administratën publike, dhe qytetarët.

Subjektet e tjera përgjegjëse për sigurinë kibernetike dhe subjektet përgjegjëse sektoriale të sigurisë së rrjeteve dhe sistemeve të informacionit janë subjektet e përcaktuara *në faqen 7, rubrika Zbatimi dhe monitorimi.*

Gjithashtu do të preken nga zbatimi i projektligjit edhe organizmat e vlerësimit të konformitetit sipas Skemës Kombëtare të Certifikimit të Sigurisë Kibernetike. Projektligji synon rregullimin e mungesës së këtyre organeve duke qenë se aktualisht nuk ka të tillë që operojnë në Republikën e Shipërisë, duke përcaktuar rregullat për akreditimin e tyre dhe funksionimin e tyre, si dhe detyrat dhe përgjegjësitë respektive sipas rastit.

**“Organet e Vlerësimit të Konformitetit”**, janë personat juridik kombëtar ose ndërkombëtar, të akredituar nga institucioni përgjegjës për akreditim, për të kryer vlerësimet dhe testimet e konformitetit të produkteve, shërbimeve dhe proceseve TIK, si dhe vlerësimin e masave të sigurisë kibernetike të implementuara nga infrastrukturat kritike dhe të rëndësishme të informacionit.

Pra, organet e vlerësimit të konformitetit kryen vlerësimet dhe testimet e konformitetit të produkteve, shërbimeve dhe proceseve TIK, si dhe vlerësimin e masave të sigurisë kibernetike të implementuara nga infrastrukturat kritike dhe të rëndësishme të informacionit.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) është institucioni përgjegjës për mbikëqyrjen e fushës së sigurisë kibernetike në Republikën e Shqipërisë.

Ndikimet për **qeverinë** janë si më poshtë:

*Ndikime të drejtpërdrejta:*

* Përmbushja e detyrimeve në kuadër të përafrimit të legjislacionit me acquis e BE-së. Kuadri i ri ligjor do përmbushë detyrimet në kuadër të përafrimit të legjislacionit me acquis duke pasur si fokus arritjen e një niveli të lartë të sigurisë kibernetike, për rrjetet dhe sistemet e informacionit në Republikën e Shqipërisë, duke përcaktuar qartë masat e sigurisë, detyrat e subjekteve përgjegjëse në fushën e sigurisë kibernetike, reagimin në raste të incidenteve apo rreziqeve kibernetike dhe duke pasur në focus zbatimin e standardeve evropiane për forcimin e sigurisë në infrastrukturat e informacionit.
* Rritja e sigurisë kibernetike të rrjeteve dhe sistemeve qeveritare të informacionit përmes procesit të certifikimit të sigurisë kibernetike sipas skemës kombëtare.
* Mundësimi i përgjigjes sa më efektive ndaj sfidave të sigurisë së rrjeteve dhe sistemeve të informacionit duke pasur një qasje gjithëpërfshirëse në nivel shtetëror dhe më gjerë në nivel ndërkombëtar, duke përfshirë krijimin e kapaciteteve minimale por njëkohësisht të larta dhe të mjaftueshme me qëllim planifikimin, shkëmbimin e informacionit, bashkëpunimin dhe detyrimet e përbashkëta të sigurisë për operatorët e infrastrukturave kritike të informacionit dhe operatorët e infrastrukturave të rëndësishme të informacionit.
* Efekte financiare në buxhetin e shtetit do jenë negative në tërësi në terma afatshkurtër. Duke qenë se projektligji përcakton tarifa në kuadër të masave administrative, efektet financiare janë pozitive në këtë rast. Por, ky projektligj ka edhe efekte financiare të tjera në buxhetin e shtetit që lidhen me kostot për ngritjen e strukturave dhe mekanizmave të parashikuara në dispozitat e këtij projektligji të cilat kanë efekt negativ në buxhetin e shtetit. Rrjedhimisht, ndikimi në buxhetin e shtetit në tërësi do të jetë negativ, pasi në terma afatshkurtër, kostot parashikohen të jenë më të larta se përfitimet. Megjithatë, sa i përket ekonomisë në tërësi dhe në terma afatgjatë, duke marrë të mirëqenë se ky projektligj do të zbatohet plotësisht dhe me efektivitet të lartë duke rritur nivelin e sigurisë kibernetike në vend, ndikimi do të jetë pozitiv, pasi në mungesë të një sigurie kibernetike të fortë në nivel kombëtar, kostot e pasojave do të ishin më të larta për qeverinë sesa investimet aktuale për garantimin dhe forcimin e sigurisë kibernetike sipas dispozitave të këtij projektligji.

*Ndikime jo të drejtpërdrejta:*

* Rritja e bashkëpunimit midis operatorëve të infrastrukturave të informacionit dhe institucioneve shtetërore, dhe bashkëpunimit ndërkombëtar.
* Përmirësimi i sigurisë kibernetike kombëtare duke garantuar strukturat, mekanizmat dhe kapacitetet e nevojshme, si dhe procedurat përkatëse.
* Përfitimet jo të drejtpërdrejta përfshijnë rritjen e punësimit të ekspertëve të sigurisë kibernetike në subjektet e tjera përgjegjëse për sigurinë kibernetike, si dhe rritjen e pagave të tyre duke qenë se ka një mungesë burimesh njerëzorë të specializuara në këtë fushë dhe konkurrenca për të rekrutuar më të mirët do të jetë e lartë.

**Subjektet e tjera përgjegjëse për sigurinë kibernetike duke përfshirë operatorët e infrastrukturave të informacioni**t do të preken nga ndërmarrja e kësaj politike, që do të ndikojë në përmirësimin e ofrimit të shërbimeve të tyre, por nga ana tjetër kjo do të shoqërohet me kosto shtesë pasi do të rriten kërkesat e sigurisë në ofrimin e këtyre shërbimeve gjë që do të kërkojë investime për rritjen e kapaciteteve teknike, njerëzore dhe financiare.

*Ndikime të drejtpërdrejta:*

* Kostot e politikës, pra investimet dhe shpenzimet që do të kryhen nga subjektet për të përmbushur detyrimet e parashikuara në këtë ligj, në lidhje me forcimin e kapaciteteve teknike dhe njerëzore, ngritjen e strukturave si CSIRT-et sektoriale dhe pranë operatorëve nëse nuk ekzistojnë, si dhe shpenzimet për zbatimin e kërkesave të reja të sigurisë në lidhje me certifikimin e sigurisë kibernetike dhe masat e tjera të sigurisë që duhet të zbatojnë.
* Kosto administrative pra kosot që rrjedhin nga kërkesat e reja të politikës dhe monitorimit sipas dispozitave të këtij projektligji, ku subjektet duhet të përshtasin produktet dhe shërbimet e tyre për të qenë në përputhje me kërkesat e këtij projektligji dhe të plotësojnë rekomandimet e lëna pas inspektimeve/auditimeve.
* Kosto buxheti ku subjeket do të duhet të parashikojnë në buxhetet e tyre të gjitha shpenzimet e nevojshme për të përmbushur kërkesat e këtij projektligji.
* Përfitimet e drejtpërdrejta përfshijnë rritjen e sigurisë së produkteve dhe shërbimeve të ofruara nga subjektet.

Gjithashtu edhe **bizneset, administrata publike dhe qytetarët** do të kenë përfitime jo të drejtpërdrejta ku do të shohin një përmirësim të dukshëm në përdorimin e shërbimeve të teknologjsë së informacionit qoftë nga sektori publik ashtu edhe ai privat, të cilat do të jenë më të sigurta. Privatësia dhe siguria e shërbimeve të marra do të rritet duke garantuar më mirë të drejtën e tyre për mbrotjen e të dhënave personale. Gjithashtu, do të kemi një rritje të bashkëpunimit dhe ndërveprimit, si dhe rritje të besueshmërisë së qytetarëve ndaj qeverisë dhe administratës publike sa i përket punës në fushën e sigurisë kibernetike.

**Ndikimet financiare**

***Kosto në buxhetin e shtetit:***

Projektligji sjell efekte financiare në buxhetin e shtetit duke rritur kostot të cilat parashikohen si vijon:

1. **Lidhur me infrastrukturën për sigurinë kibernetike**

 **Shtylla e parë** i referohet ngritjes së Qendrës Kombëtare Operacionale të Sigurisë Kibernetike, e cila shoqërohet me Server Room, Instalimin e agjentëve, një sërë platformash si platformat e monitorimit, platformat e ndarjes së incidenteve kibernetike, platformat e auditit, risku, web analyses.

Përllogaritja është bërë duke marrë në konsideratë gjithë teknologjinë, pajisjet hardware, software, licencat, sistemet,etj. Totali i përllogaritur për një periudhë 5-vjeçare është 12,258,228,000 lekë (120,000,000 dollarë).

1. **Lidhur me ngritjen dhe implementimin e standardeve**

**Shtylla e dytë** i referohet ngritjes së standardeve, implementimi i ISO 27001 në të gjitha infrastrukturat e informacionit, ngritja e menaxhimit të incidenteve.

Totali i përllogaritur për një periudhë 5-vjeçare është 1,225,822,800 lekë (12,000,000 dollarë).

1. **Lidhur me rritjen e kapaciteteve (trajnimet)**

**Shtylla e tretë** i referohet trajnimeve për rritjen e kapaciteteve.

Totali i përllogaritur për një periudhë 5-vjeçare është 3,677,468,400 lekë (36,000,000 dollarë).

Kosto do të ketë edhe për ngritjen ose rritjen e kapaciteteve teknike dhe njerëzore të CSIRT-ve Sektoriale në sektorët e mbuluar nga qeveria që nuk mund të përllogaritet në vlerë monetare pasi duhet të përcaktohet nga ata vetë sa i përket kostove financiare që do t’u sjellë ky projektligj.

Në formë tabelore, shpenzimet e detajuara për një periudhë 5-vjeçare, referuar tre shtyllave të mësipërme .

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Burimi i Financimit** |  |  |  **Viti i I** | **Viti i II** | **Viti i III** | **Viti i IV** | **Viti V** |
| **Lloji i kostos** | **Vlera totale e kostos** |
| **Buxheti Shtetit** | Kosto për infrastrukturën për sigurinë kibernetike (gjithë teknologjia, pajisjet hardware, software, licencat, sistemet, etj.) | 12,258,228,000 lekë (120,000,000 dollarë) | 467,721,500 lekë(4,578,686 dollarë) | 3,677,468,400 lekë(36,000,000 dollarë) | 2,451,645,600 lekë(24,000,000 dollarë) |
|  **Donatore** | Kosto për infrastrukturën për sigurinë kibernetike (gjithë teknologjia, pajisjet hardware, software, licencat, sistemet, etj |  | 5,661,392,500 leke(55,421,314 dollare | 0 | 0 |
| **Buxheti Shtetit** | Kosto për ngritjen dhe implementimin e standardeve | 1,225,822,800 lekë (12,000,000 dollarë) | 612,911,400 lekë(6,000,000 dollarë) | 367746840 lekë(3,600,000 dollarë) | 245164560 lekë(2,400,000 dollarë) |
| **Buxheti Shtetit** | Kosot për rritjen e kapaciteteve (trajnimet), | 3,677,468,400 lekë (36,000,000 dollarë) | 919,367,100 lekë(9,000,000 dollarë) | 919,367,100 lekë9,000,000 dollarë | 735493680 lekë(7, 200,000 dollarë) | 551620260 lekë(5,400,000 dollarë) | 551620260 lekë(5,400,000 dollarë) |

*-\*Konvertuar me kursin e këmbimit të datës 20.04.2023.*

***Kosto në buxhetin e subjekteve të tjera:***

**Kosto për operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit** sa i përket investimeve dhe shpenzimeve që do të kryhen nga subjektet për të përmbushur detyrimet e parashikuara në këtë projektligj, në lidhje me forcimin e kapaciteteve teknike dhe njerëzore, ngritjen e strukturave si CSIRT-et sektoriale dhe pranë operatorëve nëse nuk ekzistojnë, si dhe shpenzimet për zbatimin e kërkesave të reja të sigurisë në lidhje me certifikimin e sigurisë kibernetike dhe masat e tjera të sigurisë që duhet të zbatojnë.

**Kosto për operatorët e infrastrukturave kritike dhe të rëndësishme dhe bizneset që operojnë në fushën e teknologjisë së informacionit** për përshtatjen e produkteve dhe shërbimeve të tyre për të qenë në përputhje me kërkesat e këtij projektligji dhe kosto për plotësimin e rekomandimeve të lëna pas inspektimeve/auditimeve.

Lidhur me sa më sipër këto kosto nuk mund të përllogariten pasi ju përkasin operatorëve, sa investime do ju duhet të bëjnë, masat e sigurisë që duhet të shtojnë(duke qenë se projektligji parashikon forcim të masave të sigurisë kibernetike) si dhe ngritjen e mekanizmave të tjerë siç janë CSIRT sektoriale.

***Përfitime në buxhetin e shtetit*:** Miratimi i këtij projektligji parashikohet të ketë edhe efekte financiare pozitive në buxhetin e shtetit duke sjellë përfitime lidhur me vlerën e rritur të sanksioneve administrative/gjobat në rast kundërvajtje administrative nga subjektet sipas përcaktimeve të këtij projektligji.

**Ndikimet sociale:**

* Përmirësimi i ofrimit të shërbimeve dhe produkteve TIK duke rritur besueshmërinë tek publiku.
* Rritja e transparencës në lidhje me situatën e sigurisë kibernetike dhe kërcënive të mundshme përmes informimit të publikut kur ky informim është i nevojshëm, sipas procedurave të përcaktuara.
* Rritja e numrit të vendeve të punës dhe rrjedhimisht rritja e shkallës së punësismit të profesionistëve të teknologjisë dhe sigurisë kibernetike, duke rritur njëkohësisht edhe konkurrencën mes subjekteve që mund të çojë në rritjen e nivelit të pagave për të qenë më konkurrues dhe rekrutuar më të mirët.

# Arsyetimi i opsionit të preferuar

1. *Zgjidhni opsionin e preferuar, bazuar në analizë.*
2. *Shpjegoni arsyetimin tuaj.*

Opsioni i rekomanduar/preferuar është zgjedhur **Opsioni 2,** hartimi dhe miratimi i një ligji të ri “Për Sigurinë Kibernetike” pasi përmes tij arrihet:

* Adresimi dhe zgjidhja e problematikave aktuale. Projektligji plotëson mangësitë në kornizën ligjore aktuale dhe u jep zgjidhje problematikave në fushën e sigurisë kibernetike.
* Realizimi i objektivave. Përmbush të gjitha objektivat e shpjeguara më sipër duke rritur sigurinë kibernetike për shërbimet, produktet dhe proceset TIK, si dhe duke forcuar masat e sigurisë kibernetike në infrastrukturat kritike dhe të rëndësishme të informacionit.
* Përmbushja e objektivit të përafrimit të legjislacionit vendas me atë të BE-së në kuadër të procesit të integrimit.
* Rritja e bashkëpunimit kombëtar dhe ndërkombëtar me qëllim forcimin e sigurisë kibernetike kombëtare.

Autoriteti koordinon veprimtarinë e tij me institucionet e sigurisë dhe të mbrojtjes si dhe bashkëpunon me subjektet e tjera përgjegjëse për sigurinë kibernetike sipas përcaktimeve të bëra në këtë projektligj.

Gjithashtu Autoriteti bashkëpunon me autoritetet ndërkombëtare në fushën e sigurisë kibernetike, nëpërmjet marrëveshjeve të përbashkëta, në përputhje me legjislacionin në fuqi për marrëveshjet ndërkombëtare.

Në kuadër të përmbushjes së angazhimeve, në terma të sigurisë kibernetike si vend anëtar i Aleancës Euro-Atlantike (NATO) dhe Organizata për Sigurimin dhe Bashkëpunimin në Evropë (OSBE), Autoriteti koordinon dhe bashkërendon punën midis këtyre organizmave dhe institucioneve kombëtare.

Autoriteti merr pjesë në aktivitetet e grupit të bashkëpunimit të përbërë nga përfaqësues të Shteteve Anëtare të Bashkimit Evropian, Komisionit Evropian dhe Agjencisë së Bashkimit Evropian për Rrjetin dhe Sigurinë e Informacionit (ENISA) si dhe merr pjesë në forumet ndërkombëtare për çështje të sigurisë kibernetike dhe bashkëpunon me to, për rritjen e sigurisë kibernetike në vend.

* Rritja e transparencës lidhur me sigurinë kibernetike në vend dhe veprimtarinë e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit nëpërmjet forcimit të kërkesave të sigurisë, kontrollit dhe mbikëqyrjes, si dhe informimit të publikut.
* Rritja e sigurisë, efektivitetit, integritetit, dhe mbrojtjes së të dhënave personale të qytetarëve në përdorimin e shërbimeve dhe produkteve TIK, dhe për rrjedhojë rritja e besueshmërisë së qytetarëve ndaj qeverisë në lidhje me sigurinë kibernetike.

**Analiza e kosto – përfitimit (e pjesshme)**

Sipas opsioni 0 nuk ka kosto të shtuara monetare për të gjithë grupet e prekura pasi nuk kryhet ndonjë ndërhyrje dhe situata mbetet siç është.

Sipas opsionit 1, rriten kostot pasi shtohen masat që duhet të ndërmerren me qëllim rritjen e sigurisë për ushtrimin e veprimtarisë përkatëse të subjekteve të këtij proejktligji, por përsëri problemi ngelet i paadresuar. Opsioni 1 është i pamundur të realizohet për shkak të rregullave të teknikës legjislative (nënkupton ndryshimin e më shumë se 50% të dispozitave të ligjit ekzistues). Gjithashtu ky opsion mbart edhe kosto të cilat prekin qytetarët, bizneset, administratën lidhur me mundësinë e marrjes së produkteve dhe shërbimeve në një kohë sa më efektive dhe sa më të sigurtë. Pra, kostot lidhen drejtpërdrejtë me mungesën e parashikimeve ligjore të nevojshme për fushën e sigurisë kibernetike. Kostot e këtij opsioni janë të njëjta me opsionin 2.

Sipas opsionit 2, kostoja përbëhet nga efekte financiare për qeverinë dhe subjektet e tjera përgjegjëse për sigurinë kibernetike përfshirë operatorët e infrastrukturave kritike dhe të rëndësishme të infomacionit.

Opsioni 0 nuk sjell kosto financiare shtesë për Buxhetin e Shteti, kurse opsionet 1 dhe 2 sjellin kosto dhe përfitime financiare për Buxhetin e Shtetit.

Për sa i përket opsionit 2, si më i preferuari, sjell përfitime financiare sa i përket sanksioneve administrative si dhe përfitime në aspektin e rritjes së nivelit të sigurisë kibernetike kombëtare, zgjidhjes së problematikave aktuale dhe arritjes së objektivave strategjike në këtë fushë.

Ky opsion sjell edhe kosto financiare në Buxhetin e Shtetit pasi parashikon ngritjen e qendrës SOC, ngritjen dhe implementimin e standardeve si dhe rritjen e kapaciteteve.

Pavarësisht se Opsioni 2 ka kosto më të konsiderueshme se opsioni 1 duke qenë se parashikon ngritjen e strukturave dhe mekanizmave të rinj dhe rrit kërkesat e sigurisë ku kjo nënkupton më shumë investime, këto kosto do të ishin më produktive dhe efektive në aspektin e arritjes së objektivave dhe rezultateve të synuara sesa opsioni 1, që nuk do t’i adresonte siç duhet problematikat dhe mangësitë ligjore, duke krijuar potencialisht kosto të reja që nuk do të prodhonin rezultatet e dëshiruara. Opsioni 2, pra miratimi i një ligji të ri, është më i përshtatshëm edhe nga pikëpamja legjislative, si dhe u jep zgjidhje të gjitha problematikave të evidentuara në fushën e sigurisë kibernetike duke përmbushur të gjitha objektivat dhe duke rritur sigurinë e rrjeteve dhe sistemeve të informacionit në Republikën e Shqipërisë.

Për sa më sipër, përveç ndikimeve në Buxhetin Shtetit, gjithashtu një impakt të konsiderueshëm do të kenë edhe investimet që do të duhet të bëjnë këto subjekte për të përmbushur detyrimet e parashikuara në këtë projektligj, por kjo nuk mund të parashikohet në një vlerë monetare fikse dhe si pasojë nuk mund të kryhet analiza e plotë e kosto-përfitimit.

**Analiza kosto – efektivitetit**

Sipas analizës së kosto-efektivitetit, opsionet 0 dhe 1 janë opsionet më të pafavorshme pasi nuk adresojnë problematikat dhe nuk prodhohen rezultatet e synuara me efektivitet. Sipas opsionit 0, nuk ndërhyhet me ndryshim politike, gjë e cila do të sjellë si kosto krijimin e mangësive ligjore për shumë çështje të cilat nuk janë të rregulluara aktualisht si dhe mosadresimin e problematikave aktuale, që nga ana e tyre mund të krijojnë kosto të tjera financiare shtesë për buxhetin e shtetit.

Sipas opsionit 1, pavarësisht se do të kemi rritjen e investimeve me qëllim përmbushjen e detyrimeve nga të gjitha subjektet përgjegjëse për sigurinë kibernetike, nuk do të kishim adresim të të gjitha problematikave aktuale të përmendura më sipër (pjesa 2). Gjithashtu nga pikëpamja legjislative ndryshimet e reflektuara në përmbajtjen e projektligjit kalojnë 50% .

Për të dyja opsionet e sipërpërmendura, kjo kosto do të rëndojë mbi të gjitha grupet e prekura.

Opsioni nr.2 sjell kosto financiare në buxhetin e shtetit, por njëkohësisht garanton përmbushjen e objektivave të analizuara më sipër (*Pjesa 1*) . Gjithashtu sjell përfitime jo të drejtpërdrejta në terma afatgjatë që lidhen me përmirësimin e sigurisë kibernetike në nivel kombëtar.

##### **Analiza me shumë kritere**

Opsionet që merren në konsideratë janë:

**Opsioni 0** – status *quo-ja* dhe mosbërja e ndryshimeve ligjore, duke pritur që situata të vetë rregullohet, pa ndërhyrjen e pushtetit legjislativ.

**Opsioni 1** – Kryerja e ndërhyrjeve ligjore, duke ndryshuar ligjin nr. 2/2017 “Për Sigurinë Kibernetike”

**Opsioni 2** – Miratimi i një ligji të ri në fushën e sigurisë kibernetike i cili do të plotësonte kuadrin ligjor aktual dhe do adresonte problematikat ekzistuese.

**Kriteret për vlerësimin e opsioneve dhe pesha e secilit sipas rëndësisë relative:**

* + 1. Adresimi i problematikave ekzistuese - 5
		2. Ngritja e kapaciteteve teknike, ligjore dhe organizative - 4
		3. Garantimi i sigurisë kibernetike për produktete dhe shërbimet, si dhe operatorët e infrastrukturave të informacionit, duke përmirësuar efektivitetin, integritetin, sigurinë dhe besueshmërinë e tyre - 4
		4. Forcimi i bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike - 4
		5. Rritja e transparencës dhe besueshmërisë së publikut lidhur me sigurinë kibernetike në vend - 3
		6. Kostot –efektiviteti - 4

Shkalla e performancës është nga 0 në 5, ku 0 përfaqëson opsionin më pak të preferuar dhe 5 atë më të preferuarin .

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kriteret | Pesha | Opsioni 0 | Opsioni 1 | Opsioni 2 |
| Adresimi i problematikave ekzistuese  | 5 | 0 (0) | 1 (5) | 1(5) |
| Ngritja e kapaciteteve teknike, ligjore dhe organizative  | 4 | 1 (4) | 4 (16) | 4 (16) |
| Garantimi i sigurisë kibernetike për produktete dhe shërbimet, si dhe operatorët e infrastrukturave të informacionit, duke përmirësuar efektivitetin, integritetin, sigurinë dhe besueshmërinë e tyre  | 4 | 0 (0) | 4 (16) | 4 (16) |
| Forcimi i bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike | 4 | 3 (12) | 4 (16) | 4(16) |
| Rritja e transparencës dhe besueshmërisë së publikut lidhur me sigurinë kibernetike në vend | 3 | 3 (9) | 4(12) | 4 (12) |
| Kostot -efektiviteti | 4 | 3(12) | 3 (12) |  5 (20) |
| Pikët |  | 37 | 77 | 85 |

Për sa më sipër, bazuar te analiza kosto-përfitim, kosto-efektivitet, dhe analiza me shumë kritere, opsioni 2 ndonëse ka kosto më të lartë, është më efektiv dhe sjell më shumë përfitime sa i përket realizimit të objektivave dhe rezultateve.

Gjithashtu, opsioni 2 shihet si më i përshtatshëm pasi adreson problematikat aktuale, rregullon mangësitë ligjore, zgjeron rrethin e subjekteve të këtij projektligji si dhe passjell përfitime në buxhetin e shtetit në terma afatgjatë.

 Sipas analizës me shumë kritere, hartimi dhe miratimi i një ligji të ri për sigurinë kibernetike merr më shumë pikë në krahasim me opsionet e tjera.

# Çështje të zbatimit

1. *Shpjegoni se cila strukturë do të jetë përgjegjëse për zbatimin e opsionit të zgjedhur.*
2. *Shpjegoni pengesat e mundshme për zbatimin e opsionit të zgjedhur.*
3. *Përshkruani masat që do të ndërmerren gjatë zbatimit për të arritur qëllimet e politikës.*

Pas hyrjes në fuqi të projektligjit “Për Sigurinë Kibernetike”, institucionet përgjegjëse për zbatimin e këtij projektligji janë:

* Autoriteti përgjegjës për Sigurinë Kibernetike (Aktualisht AKCESK).
* Subjektet e tjera përgjegjëse për sigurinë kibernetike sipas përcaktimeve të bëra në këtë projektligj .
* Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit.

Masat e marra për arritjen e qëllimit të kësaj politike do të konsistojnë pikërisht në përcaktimin e qartë të detyrave të subjekteve përgjegjëse të sigurisë kibernetike duke e forcuar mbikëqyrjen si dhe reagimin më të shpejtë në raste të rreziqeve apo kërcënimeve kibermetike, si dhe forcimit të masave të sigurisë në rrjetet dhe sistemet e informacionit.

Zbatimi i plotë dhe efektiv i projektligjit varet nga nxjerrja dhe miratimi i akteve nënligjore në bazë e për zbatim të këtij projektligji. Autoritetet shtetërore që synohen të ngarkohen me miratimin e tyre janë Drejtori i Përgjithshëm i Autoritetit për një pjesë të akteve, si dhe Këshilli i Ministrave për rregullimin e çështjeve më të rëndësishme që kërkojnë vullnet më të gjerë politik për sanksionimin ligjor të tyre. Miratimi i këtyre akteve nënligjore synohet të bëhet brenda një periudhe prej **6 muajsh** nga hyrja në fuqi e ligjit, kohë të cilën e çmojmë të mjaftueshme për hartimin e akteve nënligjore normative cilësore dhe shteruese për aq sa ligji autorizon.

Autoriteti do të hartojë/përditësojë aktet nënligjore të propozuara në përputhje me legjislacionin e Bashkimit Europian.

Përzgjedhja e opsionit të preferuar-hartimi i një ligji të ri për sigurinë kibernetike mund të shoqërohet me pengesa, të cilat identifikohen kryesisht në momentin e fillimit të zbatimit të tij (pas hyrjes në fuqi). **Pengesat kryesore paraqiten në mënyrë të përmbledhur si më poshtë vijon:**

* + Vonesa në nxjerrjen e akteve nënligjore, pra përtej afatit të vendosur në projektligj për miratimin e tyre. Në lidhje me këtë aspekt, sqarojmë se puna për hartimin e akteve nënligjore fillon paralelisht me procesin e shqyrtimit dhe miratimit të kësaj nisme nga Kuvendi i Republikës, me qëllim shmangien e problematikës së vonesës. Megjithatë, mund të ndodhë që hartimi i disa prej akteve nënligjore të jetë kompleks apo i vështirë, nisur nga natyra dhe përmbajtja e çështjeve që duhet të rregullohen sipas delegimeve ligjore respektive. Nga ana tjetër, mund të ndodhë që procesi i konsultimit të tyre të marrë kohë më shumë për shkak të angazhimit të disa palëve në proces, vonesave në dërgimin e mendimit prej tyre, procesit të vazhdueshëm të bashkërendimit deri në rakordimin e qëndrimeve për rregullimin e çështjeve të caktuara.
	+ Përshtatja me legjislacionin e ri, për shkak të risive që ky projektligj sjell referuar shtimit të subjekteve përgjegjëse për sigurinë kibernetike, krijimit dhe përmirësimit të strukturave dhe mekanizmave ekzistues dhe të rinj, forcimit të kërkesave të sigurisë, dhe aplikimit të skemës kombëtare për certifikimin e sigurisë kibernetike.
	+ Koha që nevojitet për subjektet e këtij projektligji që të përshtaten me rregullat dhe procedurat e vendosura në këtë projektligj duke qenë se ligji sjell risi në kompetencat, operimin, ushtrimin e veprimtarisë, mënyrën e bashkëpunimit, ofrimin e produkteve, shërbimeve dhe proceseve të TIK, si dhe shtimim e detyrimeve dhe kërkesave të sigurisë.
	+ Anëtarësimi i Republikës së Shqipërisë në Bashkimin Evropian, duke qënë se disa dispozita në projektligj kushtëzohen me anëtarësimin në BE, gjë e cila do ndihmonte shumë për sa i përket forcimit të bashkëpunimit ndërkombëtar, rritjes së kapaciteteve dhe shkëmbimit të praktikave më të mira në fushën e sigurisë kibernetike.

**Disa prej masave që do të ndërmerren gjatë zbatimit për të arritur qëllimet e politikës janë:**

* Përcaktimi i rregullave të qarta që rregullojnë organizimin, funksionimin dhe veprimtarinë e CSIRT-eve sektoriale, dhe CSIRT-eve pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit me akt nën-ligjor.
* Përcaktimi i procedurave për identifikimin, klasifikimin, përshkallëzimin dhe menaxhimin e krizës kibernetike që do të përcaktohen me akt nën-ligjor.
* Përcaktimi i mënyrës së organizimit dhe funksionimit të CERT-it me akt nën-ligjor.
* Përcaktimi i Skemës Kombëtare të certifikimit të sigurisë kibernetike në përputhje me Skemat Certifikimit të miratuara nga Bashkimi Evropian, i niveleve të sigurisë së skemës kombëtare të certifikimit të sigurisë kibernetike për produktet, shërbimet dhe proceset e TIK, si dhe organeve përgjegjëse për akreditimin, certifikimin dhe vlerësimin e konformitetit të sigurisë kibernetike sipas Skemës së Certifikimit të Sigurisë Kibernetike me akt nën-ligjor.
* Përcaktimi i metodologjisë për identifikimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit e cila miratohet me urdhër të Drejtorit të Përgjithshëm të Autoritetit.
* Përcaktimi i përmbajtjes dhe mënyrave të dokumentimit të masave organizative dhe teknike të sigurisë kibernetike me rregullore që miratohet me urdhër të Drejtorit të Përgjithshëm të Autoritetit.
* Përcaktimi i llojeve dhe kategorive të incidenteve të sigurisë kibernetike të cilat prekin sistemet dhe rrjetet e informacionit, formatit, elementëve të raportimit, afateve të raportimit dhe mënyrës së dokumentimit të incidenteve kibernetike me rregullore të miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit.
* Përcaktimi i procedurës së komunikimit për informimin e publikut me urdhër të Drejtorit të Përgjithshëm të Autoritetit.
* Inspektimet dhe kontrollet periodike të veprimtarisë së operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit;
* Vlerësime të veprimtarisë së subjekteve përgjegjëse për sigurinë kibernetike në bazë të raporteve (vjetore dhe sa herë që kërkohet nga Autoritetit) të dorëzuara.
* Dhënia e rekomandimeve dhe lënia e një afati kohor të arsyeshëm nga Autoritetit për përmbushjen e tyre në rastin kur konstatohen parregullsi në ushtrimin e veprimtarisë së operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit.

**Faza e monitorimit dhe vlerësimit**

1. *Jepni një përshkrim të përmbledhur të masave të monitorimit dhe të vlerësimit.*
2. *Identifikoni kriteret/treguesit për të matur arritjen e objektivave ose progresin drejt tyre.*

Monitorimi i zbatimit të këtij projektligji do të bëhet nga Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (emërtimi me ligjin e ri do të jetë Autoriteti Kombëtar për Sigurinë Kibernetike) përmes analizave 6,12 mujore të zbatimit të ligjit dhe politikave strategjike duke marrë në konsideratë:

• Aktet nënligjore të miratuara në kuadër të veprimtarisë së subjekteve të këtij projektligji dhe ecuria e përshtatshmërisë.

• Nivelin e realizimit të planit të veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike

• Numrin e infrastrukturave të informacionit të raportuara dhe të identifikuara.

• Numrin e raportimeve të incidenteve kibernetike si dhe procedurën e zgjidhjes së tyre, koha dhe rezultatet e zgjidhjes së tyre.

• Nivelin e implementimit dhe dokumentimit të masave të sigurisë kibernetike nga infrastrukturat e informacionit.

• Raportet e vlerësimit dhe konformitetit të dorëzuara, si dhe vlerësimet nga inspektimet/kontrollet lidhur me konformitetin e veprimtarisë së subjekteve përgjegjëse për zbatimin e këtij projektligji, operatorë të infrastrukturave kritike dhe të rëndësishme të informacionit.

• Zbatueshmëria e masave rekomanduese të lëna nga Autoriteti.

• Njoftimet vullnetare të bëra nga subjektet që nuk janë klasifikuar si infrastruktura kritike apo të rëndësishme të informacionit.

Tregues të suksesit të politikës janë:

• Nurmi i i CSIRT-ve Sektoriale të ngritura.

• Numri i infrastrukturave kritike dhe të rëndësishme të informacionit të reja të identifikuara.

• Funksionimi i Qendrës SOC, qendrës kërkimore shkencore dhe akademisë së sigurisë kibernetike.

• Koha e reagimit ndaj incidenteve kibernetike të ndodhura si dhe zgjidhja efektive e tyre.

• Përmbushja e rekomandimeve/masave korrigjuese nga operatorët e infrastrukturave të informacionit brenda afatit kohor të dhënë sipas përcaktimeve në projektligj.

• Numri i organizmave të vlerësimit të konformitetit të regjistruara sipas Skemës Kombëtare të Certifikimit të Sigurisë Kibernetike nga momenti i miratimit të skemës.

• Numri i profesionistëve të kualifikuar nga diaspora, si pjesë e strukturave përgjegjëse për sigurinë kibernetike.

**Raporti i vlerësimit të ndikimit - Shtojca 2/a**

***Tabela: Vlera aktuale neto në total (VAN) - kostot dhe përfitimet me vlerë monetare të përcaktuar në milionë lekë e zbritur për 10 vjet (Vlera aktuale e kostos dhe vlera aktuale e përfitimit); krahasuar me status quo-në*.**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|   | **Viti 1**  |  **Viti 2**  |  **Viti 3**  |  **Viti 4**  |  **Viti 5**  |  **Viti 6**  |  **Viti 7**  |  **Viti 8**  |  **Viti 9**  | **Viti 10** |
| **Faktori zbritës**  |   |   |   |   |  |   |   |   |   |  |
| Kosto për buxhetin - një here | 2,000,0000,000 lek  |  5,700,076,020 lek  |  3,800,050,680 lek  |   |   |   |   |  |
| Kosto për buxhetin - në vazhdimësi |   |   |   |   |   |  |   |   |   |  |
| Kosto për bizneset - një herë  |   |   |   |   |   |   |   |   |   |  |
| Kosto për bizneset - në vazhdimësi |   |   |   |   |   |   |   |   |   |  |
| Kosto për grupet e tjera - një herë |   |   |   |   |   |   |   |   |   |  |
| Kosto për grupet e tjera - në vazhdimësi |   |   |   |   |   |   |   |   |   |  |
| **Kosto në total**  |   |   |   |   |   |   |   |   |   |  |
| **Kosto e zbritur**= Kosto në total x Faktori zbritës |   |   |   |   |   |   |   |   |   |  |
| Përfitimet për buxhetin – një herë |   |   |   |   |   |   |   |   |   |  |
| Përfitimet për buxhetin – në vazhdimësi |   |   |   |   |   |   |   |   |   |  |
| Përfitimet për grupet e tjera – një herë |   |   |   |   |   |   |   |   |   |  |
| Përfitimet për grupet e tjera – në vazhdimësi |   |   |   |   |   |   |   |   |   |  |
| Përfitimet për biznesin – një herë |   |   |   |   |   |   |   |   |   |  |
| Përfitimet për biznesin – në vazhdimësi |   |   |   |   |   |   |   |   |   |  |
| **Përfitimet totale** |   |   |   |   |   |   |  |   |   |  |
| **Përfitimi i zbritur**= Përfitimi në total x faktori zbritës |   |  |   |   |   |   |   |   |   |  |
| **Vlera prezente aktuale e përfitimit në total** |   |  |
| **Vlera prezente aktuale e kostos në total** |  |  |
| **Vlera Prezente Neto Aktuale (VAN)** = Vlera aktuale e përfitimit në total – Vlera aktuale e kostos në total |   |  |

**Raporti i vlerësimit të ndikimit - Shtojca 2/b**

***Tabelë: Vlera aktuale neto në total e çdo opsioni***

|  |  |  |
| --- | --- | --- |
| **Opsioni** | **Vlera aktuale në milionë lekë** | **Vlera aktuale neto në milionë lekë** |
| **Kosto** | **Përfitimi** |
| Opsioni 1 | -  | - | - |
| Opsioni 2 | 11,500,126,700 lekë |  |  |

**Shënim:** Përllogaritja është bërë për kostot e llogaritura në pikën Vlerësimi i opsioneve/analizimi i ndikimeve, faqja 18, për 5 vite.

Duhet të meren në konsideratë tarifat e reja që do përcaktohen si edhe organet e reja që do të akreditohen.

**KRYEMINISTRI**

[Emri Mbiemri]

1. Neni 11 i projektligjit “Për sigurinë kibernetike” [↑](#footnote-ref-1)
2. Fletorja Zyrtare e Bashkimit Evropian, Seria L, nr.194, datë 19.07.2016, faqe. 1-30 [↑](#footnote-ref-2)
3. Numri CELEX: 32016L1148, Fletorja Zyrtare e Bashkimit Europian, Seria L, nr. 194, datë 19.7.2016, faqe 1-30. [↑](#footnote-ref-3)
4. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> [↑](#footnote-ref-4)
5. Fletorja Zyrtare e Bashkimit Evropian, Seria L, nr.333, datë 27.12.2022, faqe 80-152, [↑](#footnote-ref-5)
6. <https://kryeministria.al/wp-content/uploads/2021/10/Programi_Qeverises_2021-2025.pdf>

Vendim i Këshillit të Ministrave nr.1084 datë 24.12.2020 "Për miratimin e Strategjisë Kombëtare për Sigurinë Kibernetike dhe të planit të veprimit 2020–2025 [↑](#footnote-ref-6)
7. Vendim i Këshillit të Ministrave nr.1084 datë 24.12.2020 [↑](#footnote-ref-7)