



AKCESK

**AUTORITETI KOMBËTAR PËR
CERTIFIKIMIN ELEKTRONIK
DHE SIGURINË KIBERNETIKE**

RAPORT VJETOR 2020

Tabela e Përmbledhjes

1. Drejtoria e Certifikimit Elektronik dhe Kontrollit	3
1.1 Sektori i Akreditimit dhe Politikave	3
1.2 Sektori i Komunikimit dhe Shpërndarjes së Informacionit	6
1.2.1 Aktivitete për rritjen e ndërgjegjësimit	7
1.2.2 Materiale promovuese.....	8
1.2.3 Buletinet e sigurisë kibernetike.....	13
1.3 Sektori i Kontrollit	13
2. Drejtoria e AL-CSIRT	17
2.1 Sektori i monitorimit të incidenteve kibernetike	17
2.2 Sektori i menaxhimit të incidenteve kibernetike	20
3. Sektori i financës dhe shërbimeve mbështetëse	22

1. DREJTORIA E CERTIFIKIMIT ELEKTRONIK DHE KONTROLLIT

1.1 SEKTORI I AKREDITIMIT DHE POLITIKAVE

Sektori i Akreditimit dhe Politikave ka këto përgjegjësi të përcaktuara në rregulloren e brendshme të institucionit:

- a) Shqyrton dhe vlerëson dokumentacionin përkatës dhe kërkesën e dorëzuar nga subjektet për procesin e akreditimit si ofruesi i kualifikuar i shërbimit të besuar.
- b) Mban kontakte të vazhdueshme me ofruesit e kualifikuar të shërbimit të besuar të akredituar pranë AKCESK, dhe kërkon plotësim dokumentacioni për çdo ndryshim teknik ose operacional që OKSHB ndërmerr.
- c) Menaxhon dokumentacionin e ofruesve të kualifikuar të shërbimit të besuar dhe dokumentacionin e organizmave të testimit dhe konfirmimit, si dhe mirëmban Listat e Besuara (Trust Lists) të ofruesve të kualifikuar të shërbimeve të besuara. Publikon këto lista për ndërveprim dhe njohje reciproke të nënshkrimeve elektronike me vendet anëtarë të BE-së.
- d) Raporton mbi konformitetin e dokumentacionit ligjor dhe teknik të dorëzuar nga ofruesit e kualifikuar të shërbimit të besuar, sipas kritereve të AKCESK, normave evropiane dhe standardeve teknike të ETSI (European Telecommunications Standards Institute).
- e) Vlerëson plotësimin e kritereve të Politikave të Certifikimit, të Deklaratës së Praktikave të Certifikimit, Manualit Operativ dhe Politikave të Vulës Kohore.
- f) Vlerëson dokumentacionin e dorëzuar për pajisjet e sigurta të krijimit të nënshkrimit dhe certifikatat e lëshuara nga prodhuesi i tyre, në mënyrë që të plotësohet niveli evropian i sigurisë.
- g) Harton raportin mbi kërkesën për akreditim/regjistrim të ofruesit të kualifikuar të shërbimit të besuar dhe sugjeron pranë Drejtorit të Drejtorisë, nëse subjektit duhet t'i jepet akreditimi ose jo.
- h) Harton rregulla specifike në përputhje me ndryshimet sipas standardeve ndërkombëtare, në fushën e nënshkrimit elektronik, identifikimit elektronik dhe shërbimeve të besuara dhe sigurisë kibernetike.
- i) Harton akte ligjore dhe nënligjore përsa i përket fushës së certifikimit elektronik dhe sigurisë kibernetike, sipas nevojave të evidentuara të institucionit, të harmonizuara me acquis të BE-së.
- j) Bashkëpunon dhe bashkërendon punën me institucione të tjera, për implementimin e nënshkrimit elektronik, identifikimit elektronik dhe shërbimeve të besuara.
- k) Siguron pjesëmarrjen e punonjësve, në konferenca dhe trajnime kombëtare dhe ndërkombëtare, për rritjen e nivelit profesional të punonjësve.

1.1.1 PUNËT E KRYERA GJATË VITIT 2020


Përgjatë vitit 2020 sektori i Akreditimit dhe Politikave ka realizuar detyrat e mëposhtme:

1. Në kuadër të detyrimeve të përcaktuara në legjislacionin për deklarimin e pasurisë dhe parandalimin e konfliktit të interesit, është raportuar në mënyrë periodike dhe vjetore pranë ILDKPKIE.
2. Gjatë vitit 2020 janë hartuar dhe kontribuar në hartimin e disa akteve nënligjore të brendshme të institucionit dhe të tjera të dërguara për miratim pranë Këshillit të Ministrave të cilat listohen shkurtimisht si tituj më poshtë:
 - Urdhër Nr.83, datë 01.12.2020 për një shtesë në Rregulloren mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë
 - Udhëzim nr.4, datë 10.01.2020 për “Zhvillimin e Vizitave Jashtë Vendi të Ministrave dhe Titullarëve të Institucioneve Shtetërore në Varësi të tyre dhe Kryeministrit”.
 - Ndryshim i rregullores së brendshme në përputhje me Urdhrin Nr. 6 datë 16.01.2020, Për miratimin e strukturës dhe të organikës së autoriteti kombëtar për certifikimin elektronik dhe sigurinë kibernetike.
 - Bashkë hartim i Manualit të Procedurës së Auditit në Infrastrukturat Kritike të Informacionit dhe Infrastrukturat e Rëndësishme të Informacionit
 - Harmonizim të Urdhrit nr. 80, datë 17.11.2020 “Për miratimin e rregullave dhe procedurave standarde të punës të harmonizuara, gjatë periudhës së gjendjes së epidemisë së shkaktuar nga covid-19 dhe periudhës së kohëzgjatjes së vitit shkollor 2020 – 2021”
 - Kontribut në hartimin e Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025 dhe hartim i praktikës së dokumentit.
3. Në kuadër të integritimit në Bashkimin Evropian është dhënë kontribut në këto hapësira:
 - Raportim mbi kapitujt 3 dhe 10 në kuadër të GNPIE;
 - Pjesëmarrje në takime online në kuadër të GNPIE;
 - Plotësim i pyetësorit Digital Society Trust;
 - Plotësim dhe raportim mbi PPAP dhe PKIE 2020-2022;
4. Një objektiv i rëndësishëm për sektorin dhe për institucionin, ka qenë dhe do vazhdojë të jetë edhe për vitin 2021, përditësimi i bazës ligjore në fushën e veprimtarisë së

institucionit. Ky angazhim është njëkohësisht edhe kontribut konkret dhe i rëndësishëm në rrugën e integritetit të vendit në Bashkimin Evropian.

Konkretisht ka nisur puna dhe janë në përfundim draftet paraprake sa i takon transpozimit të plotë të Rregullores Evropiane eIDAS Nr. 910/2014 “Për identifikimin elektronik dhe shërbimet e besuara për transaksione elektronike në tregun e brendshëm”, si dhe transpozimit të plotë të Direktivës (BE) 2016/1148 e Parlamentit Evropian dhe e Këshillit “Mbi masat për një nivel të lartë të përbashkët të sigurisë së rrjeteve dhe sistemeve të informacionit në të gjithë Bashkim Evropian” (NIS Directive). Këto dy akte do të prekin Ligjin nr. 9880/2008 "Për nënshkrimin elektronik", Ligjin nr. 10273/2010 "Për dokumentin elektronik", Ligjin Nr. 107/2015 "Për identifikimin elektronik dhe shërbimet e besuara", si dhe Ligjin nr.2/2017 “Për sigurinë kibernetike”.

5. Gjatë aktivitetit CyberSec 1.0, sektori ka dhënë kontribut duke marrë pjesë me një prezantim me temë Detyrimet Ligjore të OIKI dhe OIRI CSIRT - Ekipet e Përgjigjes ndaj Incidenteve Kompjuterike dhe AL-CSIRT
6. Administrimi i faqes zyrtare të Autoritetit www.cesk.gov.al. Përditësohet vazhdimisht dokumentacioni i faqes, përfshirë tekstet, ligjet, aktivitetet, lajmet më të fundit mbi qarkullimin e viruseve/vulnerabiliteteve të ndryshme në gjuhën shqipe dhe angleze.
7. Gjatë vitit 2020 është krijuar një formë raportimi në faqen zyrtare, për t’iu ardhur në ndihmë fëmijëve dhe të rinjve për raportuar përmbajtje të paligjshme apo të dëmshme të hasura gjatë lundrimit në internet.



**AUTORITETI KOMBËTAR PËR
CERTIFIKIMIN ELEKTRONIK
DHE SIGURINË KIBERNETIKE**

[Raporto Përmbajtje të Paligjshme](#) [e-Loja për Sigurinë Online](#)

[Kryefaqja](#) [Breth nesh](#) [Legjislacioni](#) [Program Transparencë](#) [Operatorët OIKI & OIRI](#)

RAPORTO PËRMBAJTJE TË PALIGJSHME

Ky shërbim ka si qëllim t'ju vijë në ndihmë fëmijëve dhe të rinjve për raportuar përmbajtje të paligjshme të hasura gjatë lundrimit në internet. Raportimet do të trajtohen me konfidencialitet të plotë nga Autoritetet Përgjegjëse për të bërë vlerësimin e rastit, si dhe për të marrë masa të menjëhershme ndaj këtyre përmbajtjeve. Fokusi ynë është krijimi i një mjedisi më të sigurt elektronik për fëmijët dhe të rinjtë në vend!

ÇFARË PËRMBAJTJE TË PALIGJSHME PO RAPORTONI?

Ekspozim ndaj imazheve të dëmshme

Cyberbullying

Pornografi me të mitur në Internet

Përmbajtje ekstremizmi i dhunshëm

Përmbajtje radikalizmi

Tjetër

KU E KENI NDESHUR KËTË PROBLEM?

Në email

Website

Në rrjete sociale

Tjetër

ADRESA WEB / URL(Uri ku keni hasur përmbajtjen e paligjshme) *

PËRSHKRIMI

8. Administrimi i sistemit të “Menaxhimit të raportimit të incidenteve të sigurisë kibernetike”, duke kryer përkatësisht hapjen e kredencialeve të personave përgjegjës të infrastrukturave kritike dhe të rëndësishme të informacionit si dhe ofrimi i asistencës teknike mbi aksesimin dhe mënyrën e përdorimit të moduleve të sistemit (për periudhën deri në Korrik 2020)
9. Pjesëmarrje në trajnime specifike për rritjen e kapaciteteve teknike dhe profesionale në fushën e Shërbimeve të Besuara organizuar nga organizmat ndërkombëtare si FESA, ENISA. Pjesëmarrje në takimin e "ENISA Article 19 Expert Group" ku u diskutua mbi marrjen e masave të duhura teknike dhe organizative për të menaxhuar riskun, për të garantuar sigurinë dhe besueshmërinë e shërbimeve të besuara si dhe mbi metodat e identifikimit elektronik në distancë.

1.1.2 PLANIFIKIMI I OBJEKTIVAVE TË SEKTORIT TË AKREDITIMIT DHE POLITIKAVE

Përgjatë vitit 2021, planifikohet realizimi i këtyre objektivave:

- Të shqyrtohen dhe vlerësohet dokumentacioni përkatës dhe kërkesat e mundshme për akreditimin e subjekteve si ofrues të kualifikuar të shërbimit të besuar.
- Hartimi i akteve ligjore dhe nënligjore, sipas nevojave të evidentuara të institucionit.
- Përfundimi i draftligjeve të harmonizuara plotësisht me Rregulloren Evropiane eIDAS Nr. 910/2014 “Për identifikimin elektronik dhe shërbimet e besuara për transaksione elektronike në tregun e brendshëm”, si dhe të Direktivës (BE) 2016/1148 e Parlamentit Evropian dhe e Këshillit “Mbi masat për një nivel të lartë të përbashkët të sigurisë së rrjeteve dhe sistemeve të informacionit në të gjithë Bashkim Evropian” (NIS Directive).

1.2 SEKTORI I KOMUNIKIMIT DHE SHPËRNDARJES SË INFORMACIONIT

Sektori i Komunikimit dhe Shpërndarjes së Informacionit ka këto përgjegjësi:

- a) Menaxhon procesin e hartimit të metodologjive të punës, për analizën e rrezikut kibernetik në OIKI/OIRI dhe mbikëqyr procesin e vlerësimit të tij.
- b) Merr pjesë në grupin e punës për vlerësimin e rrezikut kibernetik në OIKI/OIRI.
- c) Harton dhe shpërndan lajmërimi paraprake mbi sigurinë e informacionit.
- d) Analizon detyrat dhe angazhimet ndaj organizmave ndërkombëtare, në përputhje me politikatat e institucionit.
- e) Koordinon dhe përmbush detyrimet raportuese në nivel institucional mbi progresin e raportet e ndryshme.
- f) Organizon dhe bashkërendon aktivitetet e ndryshme brenda fushës së veprimtarisë së institucionit.

- g) Mban lidhje me organizmat ndërkombëtare (NATO; OSBE; FESA; ENISA; ETSI; FIRST; TI; ECSO, etj.), për përmbushjen e angazhimeve të ndërmarra nga AKCESK, në fushën e sigurisë kibernetike dhe shërbimeve të besuara.
- h) Mban lidhje me institucionet kombëtare dhe ndërkombëtare, me qëllim që të përcaktojë dhe identifikojë programet e trajnimit për rritjen e kapaciteteve të punonjësve të AKCESK dhe i propozon ato tek eprori.

Përgjatë vitit 2020 sektori ka realizuar aktivitete në kuadër të rritjes së ndërgjegjësimit të komunitetit si dhe rritjes së kapaciteteve të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, me qëllim realizimin e detyrave funksionale të Autoritetit.

1.2.1 AKTIVITETE PËR RITJEN E NDËRGJEGJËSIMIT

“Dita Ndërkombëtare e Internetit të Sigurt 2020” #CyberCorner

<https://cesk.gov.al/aktivitete/cybercorner.html>

Në kuadër të Ditës Ndërkombëtare të Internetit të Sigurt Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) në bashkëpunim me Bashkinë Tiranë dhe me mbështetjen e Raiffeisen Bank dhe Telekom Albania, lançuan projektin inovativ #CyberCorner në bibliotekën “Hamit Beqja”, pranë Njesisë Administrative Nr.8, Tiranë.

Projekti synon rritjen e ndërgjegjësimit për sigurinë e fëmijëve në Internet dhe aftësimi i tyre për përdorimin e e-shërbimeve në ambientet tashmë multifunksionale të bibliotekës “Hamit Beqja”. CyberCorner do të ofrojë për fëmijët dhe të rinjtë mundësi për njohuri të thelluara mbi tematikat aktuale dhe sensitive, si: përdorimi i internetit të sigurt, kodimi, radikalizmi dhe ekstremizmi i dhunshëm, shërbimet elektronike publike. Për secilën nga këto tema janë hartuar module, si dhe janë instaluar pajisje kompjuterike, me të cilat mund të ndërveprohet gjatë qëndrimit në ambientet e bibliotekës dhe do të organizohen nëpërmjet workshopeve nga ekspertët e AKCESK.

CyberSec 1.0

AKCESK, në cilësinë e Autoritetit përgjegjës për sigurinë kibernetike në Republikën e Shqipërisë organizoi trajnimin online “CyberSec 1.0”, për rritjen e kapaciteteve të stafit përgjegjës të CSIRT-eve sektoriale dhe studentet e TIK. Trajnimi dy-ditor siguroi një pjesëmarrje prej 35 pjesëmarrësish unikë në ditë.

Albanian Cyber Academy 4

https://cesk.gov.al/aktivitete/aca4_results.html

Edicioni i 4 i Akademisë së Sigurisë Kibernetike u organizua në datat 22 Qershor - 3 Korrik. Qëllimi i këtij aktiviteti ishte rritja e kapacitetit dhe thellimi i njohurive të profesionistëve të sigurisë kibernetike dhe studentëve të rinj të talentuar të fushës. Gjatë ACA4 morën pjesë 11

ekspertë ndërkombëtarë dhe 6 ekspertë vendas, të cilët ndanë ekspertizën e tyre me mbi 600 pjesëmarrës online dhe më shumë se 60 pjesëmarrës unikë në ditë.

Tetori – Muaji European i Ndërgjegjësimit për Sigurinë Kibernetike

AKCESK gjatë muajit tetor ka realizuar fushata ndërgjegjësimi me nxënësit e shkollave nëntëvjecare dhe të mesme të kryeqytetit me qëllim "Rritjen e nivelit të sigurisë së fëmijëve dhe të rinjve në internet". DCAF në bashkëpunim me AKCESK, UK Government dhe British Embassy në Tiranë kanë realizuar një seri videosh në gjuhën shqipe rreth Back up Data, CEO Frauds, Online Scams and Passwords për ta bërë më të kuptueshme rëndësinë e sigurisë kibernetike, nën moton "Jeta nuk është një përrallë".

Gjithashtu AKCESK ka realizuar 4 video mbi: Cyber Health, Online Safety, Cyber Hygiene, Cyberbullying. Materialet mund të gjenden në kanalin zyrtar të Autoritetit në YouTube. Në kuadër të muajit Evropian të Sigurisë Kibernetike dhe edukimit të klientit bankar, AAB ka organizuar tre Webinars. Programi u përqendrua në tema që ndihmojnë njerëzit të identifikojnë dhe të përgatiten për kërcënimet kibernetike. Fushatat vënë theksin në disa hapa të thjeshtë të cilët mbrojnë të dhënat tona personale, profesionale dhe financiare.

Gjithashtu, është organizuar seria e trajnimeve online për prindërit dhe edukatorët me temë "Siguria e fëmijëve në Internet" me mbështetjen e ITU. Trajnimet u organizuan online për pesë ditë, nga 15-19 nëntor 2020. Synimi i këtij trajnimi ishte inkurajimi i një sjelljeje më të sigurt në Internet për fëmijët dhe të rinjtë, duke theksuar këshillat për prindërit dhe edukatorët në komunikimin, suportin dhe edukimin ndaj tyre. Me rreth 100 pjesëmarrës unikë brenda dhe jashtë Shqipërisë, të cilët shfaqën interesin, entuziasmin dhe rëndësinë e rritjes së njohurive në tema të tilla, ky event arriti suksesin e tij duke motivuar dhe qenë një nxitje e vijimësisë së trajnimeve të ngjashme në fushën e TIK e jo vetëm.

Cybersec 2.0 17-18 Dhjetor 2020

AKCESK, në cilësinë e Autoritetit përgjegjës për sigurinë kibernetike në Republikën e Shqipërisë organizoi trajnimin online "CyberSec 2.0". Aktiviteti synoi rritjen e kapaciteteve dhe thellimin e njohurive në fushën e sigurisë kibernetike të operatorëve të infrastrukturave kritike të informacionit, si dhe promovimin e bashkëpunimit për ofrimin e trajnimeve specifike mbi "MDFIR Certified DFIR Specialist certification" dhe "MTIA - Certified Threat Intelligence Analyst" për anëtarët e CSIRTs sectorial në bashkëpunim me Mosse Cyber Security Institute.

1.2.2 MATERIALE PROMOVUESE

Përgjatë vitit 2020 në zbatim të planit të komunikimit të sektorit u realizua publikimi periodik i **4 posterave** dhe **8 videove promovuese** për ndërgjegjësimin e komunitetit për rritjen e nivelit të sigurisë kibernetike të realizuara me mbështetjen e DCAF.

POSTERA



Bizneset dhe sektori i bankës shpesh janë nën këto lloj kërcënimesh. Verifikoni besueshmërinë e dërguesit të postës elektronike dhe trajtoni me kujdes të dhënat e kompanisë në internet. <https://cesk.gov.al/>



Fjalëkalimet e thjeshta dhe shpërndarja e fjalëkalimeve mund të dëmtojnë sigurinë tuaj personale dhe të biznesit në internet. Përdorni fjalëkalim të fortë dhe të larmishëm, përdorni verifikimin me dy hapa. <https://cesk.gov.al/>



Ka shumë faqe interneti të reme që afrojnë blerje në internet. Sigurohuni që këto dyqane online janë të besueshme dhe të trajtojnë me kujdes të dhënat personale dhe financiare në internet. <https://cesk.gov.al/>

VIDEO PROMOVUESE

Password

👉 Si të krijomë një password të sigurt 🤖

<https://www.youtube.com/watch?v=kxRMEys3sjA&feature=youtu.be>




Perfect. Let's take that as an example. Now, replace some of letters with numbers and symbols.

YOUTUBE.COM
Passwords

Online scam

👉 Kujdes! Jeta nuk eshte nje perralle!

<https://www.youtube.com/watch?v=Y5BAbuMEAho&feature=youtu.be>



She looks tired, but happy to have finally arrived.


YOUTUBE.COM
Online scam

CEO frauds

👉 Always doublecheck first 🤖 🤖 !! ✅

#AKCESK #DCAF

<https://www.youtube.com/watch?v=9AefGaqZDZo&feature=youtu.be>



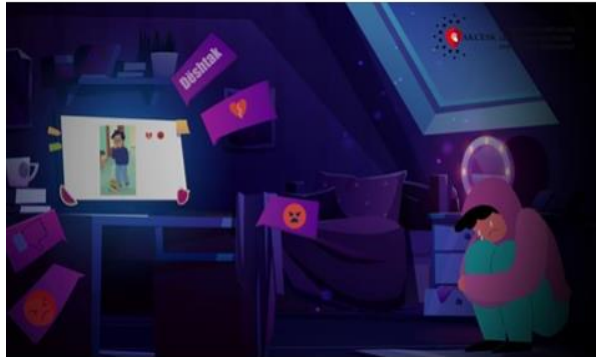
Simple.

YOUTUBE.COM
CEO frauds

Cyberbullying

👉 Injoro mesazhet kercenuese ose tallese!

<https://www.youtube.com/watch?v=0ukEJdwMIEY&feature=youtu.be>

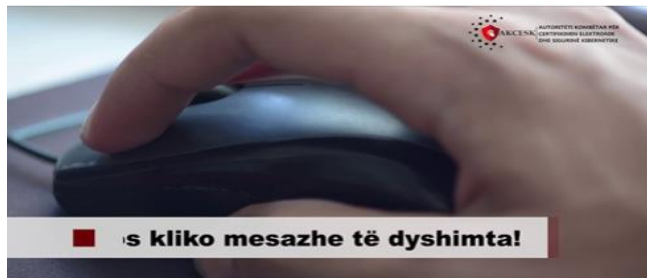


YOUTUBE.COM
Cyberbullying

Cyberhygiene

👉 APLIKO Cyber Hygiene !!

<https://www.youtube.com/watch?v=Nb-sNKGrGI&feature=youtu.be>



YOUTUBE.COM
Cyber hygiene

Për një internet më të sigurtë për fëmijët dhe të rinjtë në Shqipëri

👉 Për një internet më të sigurt për fëmijët dhe të rinjtë në Shqipëri!

<https://www.youtube.com/watch?v=TWKMybM8pbs&feature=youtu.be>



YOUTUBE.COM
PËR NJË INTERNET MË TË SIGURT PËR FËMIJËT DHE TË RINJTË NË SHQIPËRI

Online Safety

👉 Nëse ndiheni të frikësuar për sigurinë tuaj online 👤👤, kërkoni ndihmë! ✅ . #akcesk #dcaf #onlinesafety

<https://www.youtube.com/watch?v=5I7epHHAJE&feature=youtu.be>



YOUTUBE.COM
Online safety

Cyber Health

👉 Edukohu cyber !!

#thinkcyber #akcesk... See More



YOUTUBE.COM
Cyber health

Back up data

👉 !! Sa e rëndësishme është të keni kopje rezervë të të dhënave tuaja ose të biznesit tuaj ? 😞

AKCESK në bashkëpunim me DCAF kanë përgatitur për ju një video sensibilizuese. #AKCESK #DCAF #BACKUP



<https://www.youtube.com/watch?v=PYU8Fp5h54s&feature=youtu.be>



YOUTUBE.COM
Back up data
Rëndësia e back up

1.2.3 BULETINET E SIGURISË KIBERNETIKE

Çdo muaj AKCESK publikon buletin e sigurisë kibernetike me lajme dhe eventet kryesore të Autoritetit

1. [PRILL 2020](#)
2. [MAJ 2020](#)
3. [QERSHOR 2020](#)
4. [KORRIK 2020](#)
5. [TETOR 2020](#)
6. [NËNTOR 2020](#)

1.3 SEKTORI I KONTROLLIT

Sektori i Kontrollit ka këto përgjegjësi:

- a) Auditon ofruesit e kualifikuar të shërbimit të besuar (OKSHB) dhe operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit (OIKI-OIRI), në lidhje me përmbushjen e kërkesave të sigurisë, të përcaktuara sipas legjislacionit në fuqi.
- b) Kontrollon dokumentimin dhe implementimin e masave minimale të sigurisë, teknike dhe organizative, nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, në përputhje me kuadrin ligjor në fuqi dhe standardet ndërkombëtare.
- c) Përgatit, harton dhe dërgon për miratim programet e auditit të OKSHB, OIRI dhe OIKI.
- d) Menaxhon dokumentacionin e plotë të auditimeve të ofruesve të kualifikuar të shërbimit të besuar dhe operatorëve të infrastrukturave të rëndësishme dhe kritike të informacionit.
- e) Menaxhon procesin e auditeve të OKSHB-ve dhe OIKI-OIRI.
- f) Kontrollon dokumentacionin teknik të OKSHB, në mënyrë që ato të jenë të njëjta me dokumentacionin e dorëzuar pranë AKCESK.
- g) Kontrollon që OKSHB të ketë kryer, në periudhat kohore të përcaktuara, auditimet e brendshme.
- h) Kontrollon raportet e auditimit të brendshëm, shkeljet e sigurisë që janë evidentuar dhe nëse janë marrë masat e duhura për mënjanimin e tyre, pranë OKSHB dhe OIKIOIRI.
- i) Kontrollon të dhënat mbi punonjësit e zonave të sigurta dhe integritetin e tyre, pranë ofruesit të kualifikuar të shërbimit të besuar.
- j) Verifikon listat e certifikatave të kualifikuara për vlefshmërinë e tyre, pranë OKSHB.
- k) Kontrollon dhe auditon menaxhimin e aksesit të kontrollit, bazës së të dhënave, gjenerimin e çelësave, gjenerimin e certifikatave, integritetin dhe sigurinë e sistemit IT, sistemit të shfuqizimit dhe pezullimit të certifikatave, sistemin e vulave kohore, të OKSHB.
- l) Kryen rolin e audituesit të jashtëm (Organizma e Testimit dhe Konfirmimit) për OKSHB, në rastin kur nuk ka të tilla të regjistruara pranë AKCESK.
- m) Siguron funksionimin dhe përditësimin e regjistrit elektronik për procedurat e kontrollit.

- n) Propozon masa administrative në raste të evidentimit të shkeljeve ligjore, ndaj ofruesve të kualifikuar të shërbimeve të besuara dhe operatorëve të infrastrukturave të rëndësishme dhe kritike të informacionit.
- o) Menaxhon të dhëna sensitive të zotëruesve të nënshkrimeve elektronike, të cilat verifikohen gjatë auditeve pranë ofruesve të kualifikuar të shërbimit të besuar, si dhe të dhënat sensitive të OIRI dhe OIKI.
- p) Në përputhje me metodologjinë për evidentimin e infrastrukturave kritike dhe të rëndësishme, propozon nismën për rishikimin e listës së tyre.
- q) Menaxhon të dhëna statistikore mbi numrin e certifikatave të kualifikuara dhe transaksionet elektronike.
- r) Menaxhon të dhëna statistikore të përdorimit të identifikimit elektronik dhe shërbimeve të besuara, në shërbimet publike elektronike.

1.3.1 AUDITIMI I OPERATOREVE TË INFRASTRUKTURAVE KRITIKE DHE TË RËNDËSISHME TË INFORMACIONIT

Në përmbushje të detyrave funksionale, sektori i kontrollit gjatë vitit 2020, ka audituar operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit në lidhje me implementimin e masave minimale të sigurisë, teknike dhe organizative, nga këto operatorë, në përputhje me kuadrin ligjor në fuqi dhe standardet ndërkombëtare.

Konkretisht gjatë vitit 2020, Sektori i Kontrollit ka audituar, me metodën (onsite) vajtje në vend, operatorët e mëposhtëm:

1. Banka Kombëtare Tregtare
2. OTP Bank Albania
3. Banka e Parë e Investimeve
4. Agjencia Kombëtare e Shoqërisë së Informacionit.

Për infrastrukturat e reja kritike dhe të rëndësishme të informacionit të miratuara me VKM Nr.553, datë 15.7.2020, AKCESK, duke konsideruar dhe vështirësitë si rezultat të periudhës së Covid 19, filloi procesin e auditimit nëpërmjet metodës së vetë deklaramit. Thirrjes së AKCEK për vetë deklaram gjatë vitit 2020, duke plotësuar formularin e vetë deklaramit, i janë përgjigjur operatorët e mëposhtëm:

1. Korporata Elektroenergjitike Shqiptare
2. Fondi Besa sh.a
3. Sivig
4. SHKK "FED invest"
5. Eurosig.

Procesi i auditimit me vetë deklaram për operatorët që nuk kanë deklaram në vitin 2020 do të vijojë gjatë vitit 2021. Me qëllim identifikimin e infrastrukturave të reja, kritike dhe të rëndësishme të informacionit, sektori kontrollit ka nisur procesin e identifikimit të operatoreve potencial në sektorin e shëndetësisë dhe në sektorin e energjisë.

Konkretisht i janë dërguar shkresat për identifikim nëpërmjet indikatorëve përkatës 53 operatoreve që operojnë në fushën e shëndetësisë, (klinika, laborator etj..) si dhe 31 operatoreve që operojnë në fushën e energjisë. Sipas informacioneve që do dërgohen nga këto operator, AKCESK do të vijojë me procesin e klasifikimit të tyre si kritik ose të rëndësishëm.

1.3.2 AUDITIMI I OFRUESVE TË KUALIFIKUAR TË SHËRBIMIT TË BESUAR

Në përmbushje të detyrave funksionale sektori i kontrollit gjatë vitit 2020, ka audituar Ofruesit e Kualifikuar të shërbimit të besuar (OSHB), që operojnë në Republikën e Shqipërisë në zbatim të kuadrit ligjor përkatës. OKSHB ka detyrimin të raportoje periodikisht pranë AKCESK.

Gjatë vitit 2020, Sektori i Kontrollit ka mbikëqyrur veprimtarinë e OKSHB ALEAT në 82 zyrat e regjistrimit dhe shpërndarjes së certifikatave të kualifikuara në Republikën e Shqipërisë.

OKSHB ALEAT

OKSHB ALEAT gjatë vitit 2020 ka realizuar veprimtarinë si më poshtë:

Pajisja me E-Certifikata

Procesi i pajisjes me e-Certifikata në Zyrat Qendrore të Aleat vazhdon që prej 1 Janar 2014. Pajisja me e-Certifikata gjithashtu përformohet në zyrat e Aleat, në 36 qarqe të Shqipërisë.

Letërnjoftimet e-ID të certifikuara paraqiten në grafikët e mëposhtëm për vitin 2014 deri më 2020, së bashku me një raport mujor për vitin 2020. Aleat ka bërë të mundur që deri në fund të Dhjetorit 2020, të aktivizohen me këtë shërbim një total prej **2,215.726** letërnjoftime e-ID.

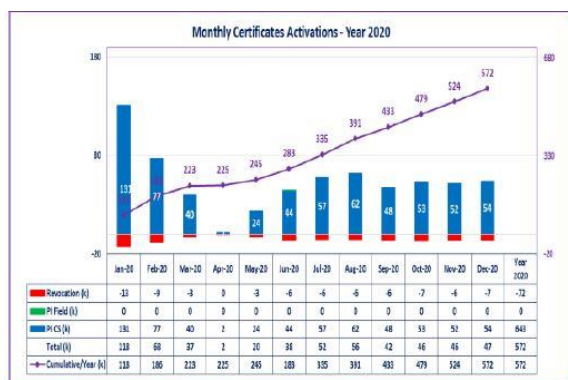


Fig. 1: Aktivizimi i Letërnjoftimit E-ID për muaj (Jan - Dhjet 2020)



Fig. 2: Aktivizimi i Letërnjoftimit E-ID sipas viteve dhe Kumulativi

Lista e Shfuqizimit të e-Certifikatave

Një total prej **268.542** Certifikatash janë revokuar deri në fund të muajit Dhjetor 2020, duke përfaqësuar rreth **12%** të totalit të letërnjoftimeve ID të aktivizuara. Totali për muaj (Viti 2020) dhe totali për të gjithë periudhën (Viti 2014, 2015, 2016, 2017, 2018, 2019 dhe 2020 për referencë) Letërnjoftimeve eID të revokuara paraqitet në grafikun më poshtë.

Revokimi i certifikatave ndodh kryesisht për shkak të zëvendësimit të Letërnjoftimit ID, të pajisur me certifikatë (pas vitit 2014).

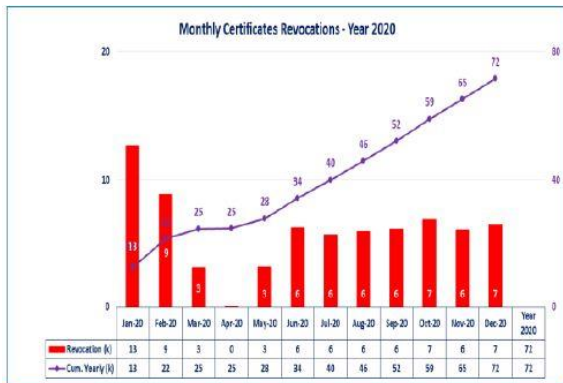


Fig. 3: Revokimi i Letërnjoftimit e-ID për muaj (Jan - Dhjet 2020)

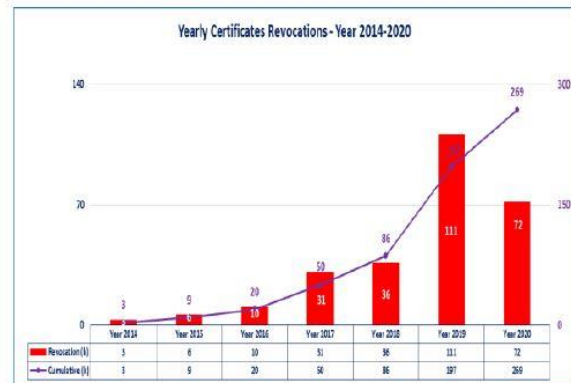


Fig. 4: Revokimi i Letërnjoftimit e-ID sipas viteve dhe Kumulativi

Totali i e-Certifikatave

Aleat ka kryer me sukses aktivizimin me Certifikata Elektronike të rreth **2,215.726** (2,484.268 aktivizime – 268.542 revokime) të letërnjoftimeve ID deri në fund të Dhjetor 2020.

2,215.726 Letërnjoftimet ID të aktivizuara përmbajnë certifikata të vlefshme dhe përfaqësojnë rreth **63.3%** të Letërnjoftimeve ID.

Aktivitete të përformuara përgjatë Tremujorit të Katërt / 2020

Për sa i përket aktiviteteve të përformuara në tremujorin e katërt të 2020, vlen për tu përmendur se në datën 10 Dhjetor 2020, është kryer rinovimi i certifikatës së eIDAS & ETSI për Aleat.

Zhvillimet në Sektorin Privat

Aktualisht, Aleat ka nënshkruar 11 (njëmbëdhjetë) marrëveshje për Projekte Pilot. Aktualisht 7 (shtatë) prej tyre operojnë Live me një total prej 70 degësh:

- Raiffeisen Bank (13 degë),
- OTP Bank (6 degë), Union Bank (3 degë),
- NOA (10 degë), Intesa Sanpaolo Bank (34 degë),
- Kredo Finance (3 degë)
- Austrian Institute of Excellence (1 degë).

Ndërkohë 4(katër) janë gati për të filluar: AADF, BKT, Posta Shqiptare dhe ACER Albania. Easy Pay, Fed Invest dhe Dhoma Kombëtare e Noterëve janë në statusin e pritjes.

Gjatë Tremujorit të Katërt të 2020, janë kryer rreth **6,132 transaksione**, duke arritur një total prej **172,667 transaksionesh** të suksesshme që nga lançimi i shërbimit në vitin 2016.

OKSHB AKSHI

OKSHB AKSHI gjatë vitit 2020 ka realizuar veprimtarinë si më poshtë:

Gjatë vitit 2020 nga AKSHI janë lëshuar 2628 certifikata me nënshkrim elektronik për administratën publike, 1624 certifikata me nënshkrim elektronik për biznesin (fiskalizimi) si dhe 3381 certifikata për sistemin e-receta.

Janë lëshuar gjithashtu nga OKSHB AKSHI 5519 certifikata për e-leje dhe agjentet doganore.

2. DREJTORIA E AL-CSIRT

2.1 SEKTORI I MONITORIMIT TË INCIDENTEVE KIBERNETIKE

Objektivat e Sektorit të Monitorimit të incidenteve kibernetike :

- a. Kryen detyrat në përputhje me aktet ligjore e nënligjore në fuqi, sipas përshkrimit të vendit të punës dhe është përgjegjës për punën që i ngarkohet.
- b. Merr pjesë në grupin e punës për monitorimin e Infrastrukturat Kritike dhe të Rëndësishme të Informacionit në lidhje me evidentimin e dëmeve dhe mangësive në zbatimin e standardeve teknike
- c. Kryen analizimin, implementimin e politikave të sigurisë për sisteme dhe rrjete të informacionit.
- d. Monitoron sistemet/ rrjetet nga aksesit i paautorizuar, modifikimi i pa lejuar i të dhënave apo shkatërrimi i tyre.
- e. Kryen kërkime të vazhdueshme mbi zhvillimet në fushën e sigurisë kibernetike; dhe rekomandon upgrade sigurie në rastin e konstatimeve të vulnerabiliteteve.
- f. Prodhon raporte periodike ose ad-hoc të një cilësie të lartë për incidente, kërcënime sigurie dhe cenueshmërie
- g. Zhvillon marrëdhënie bashkëpunimi me sektorët e tjerë të drejtorisë dhe të institucionit
- h. Jep kontribut në përgatitjen e akteve ligjore dhe nënligjore, për sa i përket fushës së veprimtarisë së Autoritetit .
- i. Planifikon, ekzekuton, vlerëson dhe monitoron të gjitha detyrat e përcaktuara në kuadër të CSIRT-it Kombëtar.

Për vitin 2020 sektori i monitorimit të incidenteve kibernetike ka realizuar detyrat si më poshtë:

1. Në zbatim të ligjit 2/2017, "Për sigurinë kibernetike" sektori ka realizuar gjithë procesin e punës për miratimin e vendimit të Këshillit të Ministrave, deri në draftimin e Vendimit nr. 553, datë 15.07.2020, "Për miratimin e Listës së Infrastrukturave Kritike të Informacionit dhe të Listës së Infrastrukturave të Rëndësishme të

Informacionit", për sektorin publik dhe sektorin privat, bazuar në standardet ndërkombëtare për sigurinë kibernetike. Në VKM e sipërpërmendur ka bërë ndryshime në emërtime të infrastrukturave kritike dhe të rëndësishme të informacionit si dhe ka shtuar dhe hequr infrastruktura të reja kritike dhe të rëndësishme të infomacionit sipas tabelës si më poshtë:

<u>OIKI</u>	SISTEME	RRJETE
ENERGJITIK	5	0
SHËNDETËSIA	5	0
FINANCIAR	1	2
TRANSPORTI	5	0
QEVERITAR	19	5
INFRASTRUKTURA DIXHITALE	4	0
Total	39	7
<u>OIRI</u>		
TRANSPORTI	ËSHTË HEQUR 1	
SHËNDETËSIA	JANË HEQUR 7	
FINANCIAR	25	
QEVERITAR	5	
INFRASTRUKTURA DIXHITALE	1	
Total	31 - 8	

2. Ka realizuar administrimin e Portalit Online për mbylljen e aksesit të faqeve me përmbajtje të paligjshme, ka dhënë suport për institucionet, për aksesimin e Portalit Online. Agjencia Shtetërore për Mbrojtjen e të Drejtave të Fëmijëve gjatë vitit 2020 ka raportuar në Portalin Online 36 faqe me përmbajtje të paligjshme të cilat janë evidentuar në rrjetet sociale dhe youtube .
3. Në bazë të ligjit Nr. 2/2017 për “Sigurinë Kibernetike”, neni 6, pika 2, Këshilli i Ministrave, miraton listën e infrastrukturave kritike të informacionit dhe të infrastrukturave të rëndësishme të informacionit, e cila përditësohet të paktën një herë në dy vjet. Për bërë të mundur që institucionet të kishin më të lehtë identifikimin dhe klasifikimin e infrastrukturave kritike dhe të rëndësishme të informacionit, sektori ka hartuar dhe miratuar versionin 1.1 “Metodologjia për Identifikimin dhe Klasifikimin e Infrastrukturave Kritike dhe Infrastrukturave të Rëndësishme të Informacionit”.

4. Numri i incidenteve të raportuara nga brenda dhe jashtë Shqipërisë deri në maj 2020 është sipas tabelës më poshtë:

	Institucioni ku ka ndodhur incidenti	Njoftuar AKCESK	Lloj i incidentit
1	Bashkia Tirane	07.01.2020	Unauthorised release of or disclosure of information
2	Misioni i Shqipërisë në USA	14.01.2020	3 email-e fishing
3	Ministria e Jashme	14.01.2020	3 email-e fishing
4	Cert Grek	22.01.2020	Malicious Activity Notification (Disa IP)
5	Word Bank Group	17.03.2020	fishing email nga ASP
6	Cert i Italisë	16.03.2020	fishing email nga sallaoperativegjrokaster@ASP.gov.al)
7	Cert i Ruisë	16.03.2020	DDoS attacks nga IP te Shqiperise
8	Cert i Finlandës	25.03.2020	dergon spame nga email I ASP
9	Netcraft Takedown Service	24.03.2020	fishing site nga Shqiperia
10	Certi Sllovak	24.03.2020	fishing email nga sallaoperativegjrokaster@ASP.gov.al)
11	Tirana Bank	15.05.2020	aktivitet Fraud me Kartat e Debitit

5. Riidentifikimi dhe klasifikimi i infrastrukturave kritike dhe të rëndësishme të informacionit.
6. Pjesëmarrja në webinare të organizuar nga Këshilli i Europës, OSCE, dhe Carnegie Mellon University në kuadër të ngritjes së kapaciteve me tema:
- Kripto për Autoritetet e Drejtësisë Penale,
 - Grupi i Punës i Ballkanit Perëndimor,
 - Ligjet Ndërkombëtar të Operacioneve Kibernetike.
7. Në kuadër të ngritjes së kapaciteve dhe në kuadër të CyberSec1.0 dhe CyberSec 2.0 të organizuar nga AKCESK për Operatorët e Infratrakturave Kritike të Infomacionit dhe Operatorët e Infrastrukturave të Rëndësishme të Informacionit , janë realizuar dy tema:
- Metodologjia për Identifikimin dhe Klasifikimin e Infrastrukturave Kritike dhe të Rëndësishme të Informacionit.
 - Investigimi me burime të hapura

2.2 SEKTORI I MENAXHIMIT TË INCIDENTEVE KIBERNETIKE

2.2.1 OBJEKTIVAT

- a) Realizimi i monitorimit të sistemit mbi raportimin dhe menaxhimin e incidenteve kibernetike, në Infrastrukturave Kritike dhe të Rëndësishme të teknologjisë së informacionit.
- b) Bashkërendimi i punës për zgjidhjen e incidenteve të sigurisë kibernetike me operatorët përgjegjës në fushën e sigurisë kibernetike kombëtare dhe ndërkombëtare.
- c) Kryerja e kërkimeve të vazhdueshme mbi zhvillimet në fushën e sigurisë kibernetike dhe rekomandon përditësime sigurie në rastin e konstatimeve të vulnerabiliteteve.
- d) Pjesëmarrja në grupe të ndryshme pune.
- e) Koordinimi i punës me sektorët e tjerë për te realizuar trajnime periodike për CSIRT-et sektoriale, me qëllim rritjen e kapaciteteve profesionale të tyre.

A) Gjatë vitit 2020 janë raportuar nga OIKI/OIRI apo dhe nëpër informacione të marra nëpërmjet partnerëve apo palëve të treta 26 Incidente Kibernetike:

- Card Fraud – Tirana Banka
- Sistemi “Mësues Për Shqipërinë” – Malicious Software
- Sistemi “Albsrep” i ASHK – vulnerability / weakness
- Sistemi “Core Router” i Abissnet – DdoS
- Card Fraud – Disa Institucione Financiare (Banka)
- Phishing Attack – Sistemi i Emalit (AKSHI/AKCESK)
- Phishing Campaign Attacks, mbi 20 drejtuar OIKI/OIRI dhe bizneseve te tjera

Ekipi i Menaxhimit të Incidenteve në bashkëpunim edhe me sektorët e tjerë të AKCESK ka marrë të gjitha masat për reduktimin e impaktit të këtyre incidenteve në momentin e ndodhjes si dhe masa të tjera korrigjuese dhe ndërgjegjësuese në të gjithë operatorët për parandalimin e sulmeve të ngjashëm.

B) Duke shfrytëzuar marrëveshjet e bashkëpunimit MoU me Cirt’et rajonale dhe ato ndërkombëtare është kryer komunikimin i vazhdueshëm me këto ekipe për bashkëpunim në incidentet e ndodhura dhe ato të mundshme të cilat kanë afektuar apo mund të afektojnë Operoret e Infrastrukturave Kritike dhe të Rëndësishme në Republikën e Shqipërisë.

C) Duke bashkëpunuar me partnerë ndërkombëtarë si:

- Qualys
- EATM Cert
- Shadowserver

dhe me sektorët e tjerë të AKCESK (sektori i Kontrollit) janë prodhuar dhe publikuar në interval kohor (javor dhe 2-javor) të rekomandimeve si dhe vulnerabiliteteve të evidentuara të sistemeve TIK. Këto raporte përditësimi u janë dërguar OIKI dhe OIRI me anë të Sistemit të Monitorimit dhe Menaxhimit të Incidenteve si dhe nëpërmjet e-mailit zyrtar të institucionit për ata operatorë të cilët kanë hasur problem në aksesimin e sistemit.

Sektori i Menaxhimit të Incidenteve në bashkëpunim edhe me sektorët e tjerë të AKCESK, ka prodhuar dhe publikuar:

- Rekomandime për Sigurinë në Internet kur Punoni nga Shtëpia për Punëdhënësit dhe Stafin
- Rekomandime për Sigurinë në Internet për Blerje Shitje Online për Qytetaret dhe Bizneset
- Rekomandime dhe Këshilla për Përdorimin e platformës ZOOM
- Rekomandime mbi Sulmet Phishing
- Njoftime mbi Sigurinë/ Security Update
- Rekomandimi për Kujdes nga kriminelët që pretendojnë të jenë WHO
- Vulnerability Alert - Adobe ka lëshuar 21 "Patche" kritike në Illustrator dhe Bridge
- Vulnerabilitet "zero day" në IOS
- CVE-2020-0796 SMBv3 Vulnerability
- Betternet & PrivateVPN
- Vulnerabilitet në Microsoft Teams
- Vulnerabilitete në librarinë Autodesk FBX në Word dhe Office
- Tre vulnerabilitete kritike në Mozilla Firefox
- Produktet Sophos XG Firewall, viktime të një sulmi zero-day
- Vulnerabilitet XSS në VMware ESXI

D) Pjesëmarrje në grupet e ndryshme të punës në dhënien e asistencës për kryerjen e detyrave për secilin sektor kryesisht në kryerjen e detyrave të auditit së bashku me Sektorin e Kontrollit.

Vlen të theksohet bashkëpunimi me të gjithë sektorët e AKCESK për marrjen e Statusit:

- "Accredited Member" nga Trusted Introducer ne 27 Maj 2020.
- "Fellow Member" nga FIRST (Forum for Incident Response Teams) 24 Shkurt 2020

E) Ngritja e kapaciteteve profesionale për nevoja të brendshëm dhe OIKI /OIRI

- SANS Institute : Reverse Engineering Malware – Malware Analysis Tools and Techniques
- Carnegie Mellon - Western Balkans Working Group, Steps for Creating National CSIRT
- Cybersec 1 dhe 2 : Hyrje ne ISO 27001, Social Engineering, Hack the Box, Menaxhimi i Incidenteve Kibernetike
- Cyberdrill : Së bashku me Silensec me Platformën "CyberRange"

3. SEKTORI I FINANCËS DHE SHËRBIMEVE MBËSHTETËSE

Për Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike buxheti i alokuar për vitin 2020 është 50,203 mijë lekë nga të cilat 46,203 mijë lekë Shpenzime Korrente dhe 4,000 mijë lekë Shpenzime Kapitale me financim të brendshëm.

Në vijim paraqesim më të detajuar realizimin e shpenzimeve sipas fondeve të alokuara:

Llogaria	Totali	Realizimi	%
600	28,664,000	19,410,482	68%
601	3,939,000	3,104,568	79%
602	13,240,000	13,240,000	93%
605	260,000	190,350	73%
606	100,000	-	0%
231	4,000,000	2,873,964	72%
Shuma	50,203,000	37,845,665	68%

Fondi i Pagave dhe Sigurimeve Shoqërore (zërat 600+601) Shumat e alokuara për paga dhe sigurime shoqërore për vitin 2020 janë përkatësisht 28,664,000 lekë për artikullin 600 dhe 3,939,000 lekë për artikullin 601. Dhe realizimi është përkatësisht 19,410,482 lekë për artikullin 600 dhe 3,104,568 lekë për artikullin 601.

Fondi për shpenzime në mallra dhe shërbime (zëri 602) Shuma e alokuar për vitin 2020 për shpenzime operative është 13,240,000 lekë. Dhe realizimi për këtë artikull është 13,240,000 lekë.

Fondi për transferimet korrente jashte (zëri 605) Shuma e alokuar për vitin 2020 për shpenzime operative është 260,000 lekë. Dhe realizimi për këtë artikull është 190,350 lekë.

Fondi i Veçantë (zëri 606) Shuma e alokuar për vitin 2020 për shpenzime për ndihma në fatkeqësi është 100,000 lekë. Dhe realizimi për këtë artikull është 0 lekë.

Fondi për Investime të brendshme (zërat 230+231), është miratuar në shumën 4,000,000 lekë në zërin 231. Dhe realizimi për këtë artikull është 2,873,964 lekë.

AKCESK në fillim të vitit 2020, konkretisht me Urdhrin e Kryeministrit Nr. 6, datë 16.01.2020 miratoi strukturën e re. Me strukturën e re u shtuan dhe 7 pozicione te reja dhe numri i planifikuar i stafit arriti në 24. Gjatë vitit 2020 kemi bërë rekrutime të reja duke e shtuar numrin e stafit me 4 persona.