



**AKCESK**

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

# **RAPORT VJETOR 2022**

Rr. "Papa Gjon Pali II", Nr. 3, Kati I  
Tiranë, Shqipëri

## Tabela e përmbledhjes

1. Drejtoria e Certifikimit Elektronik dhe Kontrollit .....	1
1.1 Sektori i Akreditimit dhe Politikave .....	1
1.2 Sektori i Komunikimit dhe Shpërndarjes së Informacionit.....	2
1.2.1 Monitorimi i “Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025” .....	2
1.2.2 Aktivitete për rritjen e ndërgjegjësimit .....	4
1.2.2 Materiale promovuese.....	7
1.2.3 Buletinet e sigurisë kibernetike .....	9
1.3 Sektori i Kontrollit .....	12
1.3.1 Auditimi i Ofruesve të Kualifikuar të Shërbimit të Besuar.....	13
1.3.2 Vlerësimi i sigurisë nëpërmjet masave emergjente të sigurisë kibernetike .....	14
1.3.3 Vlerësimi i riskut të sigurisë kibernetike.....	14
1.3.4 Hartimi i kuadrit të ri ligjor .....	15
2. Drejtoria e AL-CSIRT.....	15
2.1 Sektori i monitorimit të incidenteve kibernetike .....	15
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

#### **Përgjatë vitit 2022 sektori i akreditimit dhe politikave ka realizuar detyrat e mëposhtme:**

1. Në kuadër të integritit të vendit në Bashkimin Evropian ka vazhduar puna për përditësimin e bazës aktuale ligjore, ku përfshihen Ligji nr. 9880/2008 "Për nënshkrimin elektronik", Ligjin Nr. 107/2015 "Për identifikimin elektronik dhe shërbimet e besuara", si dhe Ligjin nr.2/2017 "Për sigurinë kibernetike" në harmonizim të plotë me Rregulloren Evropiane eIDAS Nr. 910/2014 "Për identifikimin elektronik dhe shërbimet e besuara për transaksione elektronike në tregun e brendshëm", si dhe në harmonizim të plotë me Direktivën (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).

Lidhur me ecurinë e dy projektligjeve, Projektligji "Për identifikimin elektronik dhe shërbimet e besuara" dhe paketa shoqëruese është nxjerrë për konsultim publik më datë 07.12.2022, proces i cili ka përfunduar më datë 10.01.2023. Projektligji është duke u rishikuar në bazë të komenteve të sjella nga institucionet dhe subjektet e interesuara. Afati për dorëzimin e këtij projektligji është planifikuar 3 mujori i parë i vitit 2023.

Për projektligjin "Për Sigurinë Kibernetike" është hartuar drafti final i projektligjit, por me miratimin e Direktivës NIS2 në dhjetor të 2022, me qëllim përfshirjen e disa elementëve të kësaj Direktive është bërë rishikimi i projektligjit. Për sa i përket ecurisë së projektligjit është duke u përgatitur paketa e plotë për të vijuar më tej me procedurat përkatëse për konsultim publik. Afati i planifikuar për dorëzimin e këtij projektligji është tremujori i parë i vitit 2023.

2. 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 ILDKPKI.
3. Gjatë vitit 2022 janë miratuar:
  - "Rregullore mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë kibernetike" - miratuar me urdhër të Drejtorit të Përgjithshëm nr. 10, datë 14.02.2022.
  - "Metodologji për Identifikimin dhe Klasifikimin e Infrastrukturave Kritike dhe Infrastrukturave të Rëndësishme të Informacionit", miratuar me urdhër të Drejtorit të Përgjithshëm nr.9, datë 14.02.2022.
  - VKM Nr. 553, datë 15.7.2020 "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit", ndryshuar me VKM Nr. 761, datë 12.12.2022.
  - Kontribut në procesin e identifikimit të infrastrukturave kritike të informacionit dhe infrastrukturave të rëndësishme të informacionit (pjesë e grupit të punës)

4. Kontribut me informacione dhe raportime të vazhdueshme lidhur me ecurinë e zbatimit të masave dhe aktivitetet e parashikuara në planin e veprimit 2021-2023 të “Strategjisë ndër sektoriale të luftës kundër terrorizmit 2021- 2025”.
5. Kontribut lidhur me hartimin e dokumentit strategjik në fushën e parandalimit dhe kundërshtimit të ekstremizmit të dhunshëm P/CVE të “Strategjisë së re për Parandalimin dhe Kundërshtimin e Ekstremizmit të Dhunshëm 2022-2026”
6. Në kuadër të integritimit në Bashkimin Evropian është dhënë kontribut në këto hapësira:
  - Raportim mbi kapitujt 3, 10, 24 në kuadër të GNPIE;
  - Pjesëmarrje në takime në kuadër të GNPIE;
  - Plotësim dhe raportim mbi PPAP dhe PKIE 2022-2024; PKIE 2023-2025;
7. Pjesëmarrje në trajnime për rritjen e kapaciteteve teknike dhe profesionale në fushën e shërbimeve të besuara dhe sigurisë kibernetike organizuar nga FESA, ENISA, etj.
8. Pjesëmarrja në konferencën “Speakers at Montenegro”, CCB conference, 9 Maj 2022 (pjesë e panelit si folës dhe raportues).
9. Pjesëmarrja në workshop “CRDF Global Cross Cyber Drill “– 7 July and 8 July 2022”; TAIEX Expert Mission on Request for transposition of regulatory framework in Cyber Security with NIS directive, 20.07.2022, workshop “The implementation of EU Cybersecurity Law” 14-15 Dhjetor, EGA.
10. Hartim raportesh ligjore si dhe korrespondenca shkresore të ndryshme me institucionet sipas nevojës.

## 1.2 Sektori i Komunikimit dhe Shpërndarjes së Informacionit

### 1.2.1 Monitorimi i “Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025”

Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025 u miratua me Vendimin nr. 1034 datë 24.12.2020, të Këshillit të Ministrave dhe përbën një instrument kyç për rritjen e sigurisë së rrjeteve dhe sistemeve të informacionit në nivel kombëtar dhe prioritet i Qeverisë Shqiptare.

Me kontributin e aktorëve të strategjisë është hartuar raporti i parë i monitorimit të strategjisë, i cili ka për qëllim të vlerësojë ecurinë e zbatimit të kësaj strategjie sipas 4 qëllimeve të politikave dhe objektivave respektive për periudhën Janar – Dhjetor 2021.

Plani i Veprimit i Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025 përfshin në total 125 aktivitete bazë për t’u implementuar përgjatë viteve të zbatimit të Strategjisë.. Nga këto 52% (65 aktivitete) janë realizuar plotësisht përgjatë vitit të parë 2021, ndersa 42% (52 aktivitete) pritet të fillojnë përgjatë vitit 2022 e me pas.

Në veçanti ka progres në përbushje të qëllimit të politikës së parë mbi “Garantimin e sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit, duke fuqizuar mjetet teknologjike dhe juridike” po të konsiderohen aktivitetet e realizuara dhe ato që janë në proces.

Në realizimin e objektivave të kësaj politike janë parashikuar 49 aktivitete (39%), 29 prej të cilave të realizuara plotësisht dhe 8 në proces siç shihet në grafikun mëposhtë:

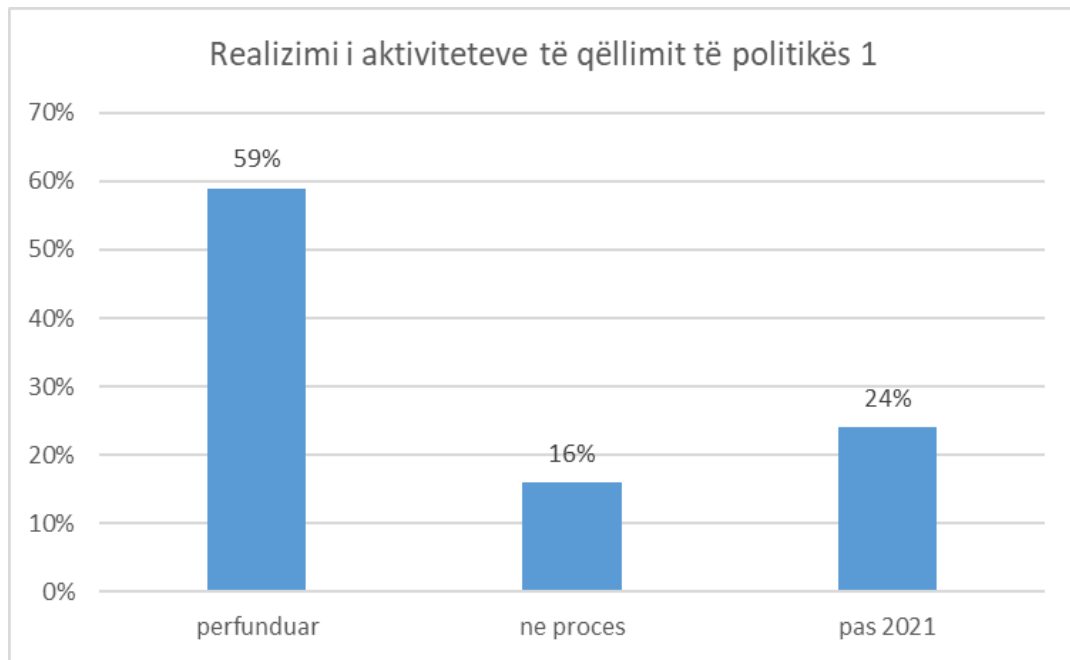


Figure 1 Realizimi i aktiviteteve të qëllimit të politikës 1

Në realizimin e objektivave të qëllimit të politikës së dytë janë parashikuar 19 aktivitete (15%), 8 prej të cilave të realizuara plotësisht dhe 11 të pafilluara akoma siç shihet në grafik.

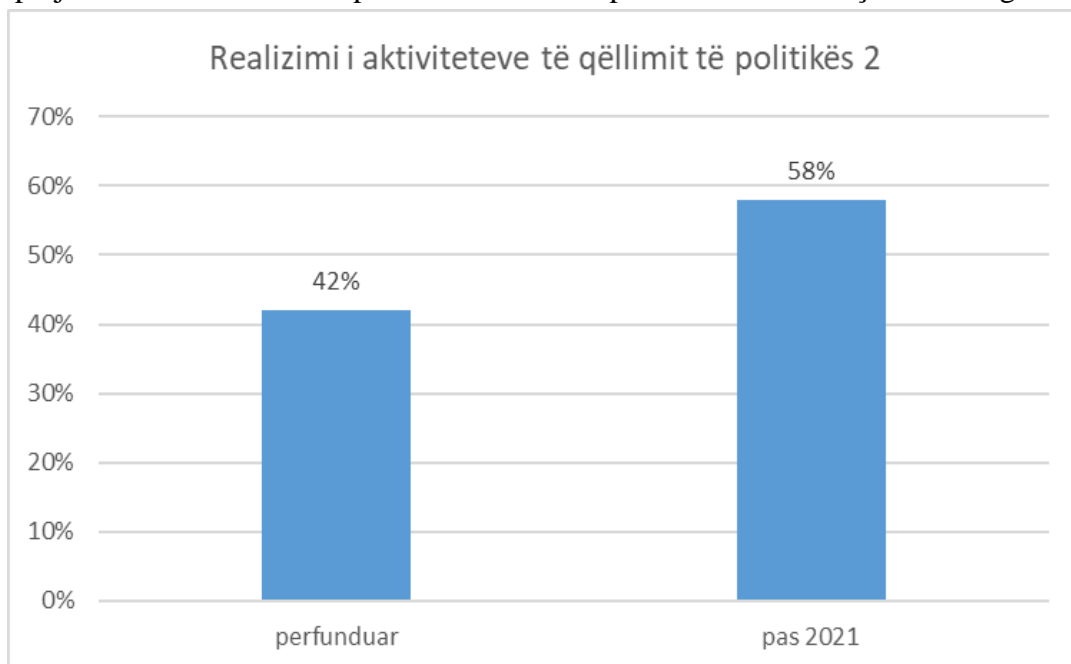


Figure 2 Realizimi i aktiviteteve të qëllimit të politikës 2

Në realizimin e objektivave të qëllimit të politikës së tretë janë parashikuar 42 aktivitete (34%), 17 prej të cilave të realizuara plotësisht dhe 25 të pafilluara akoma siç shihet në grafik.

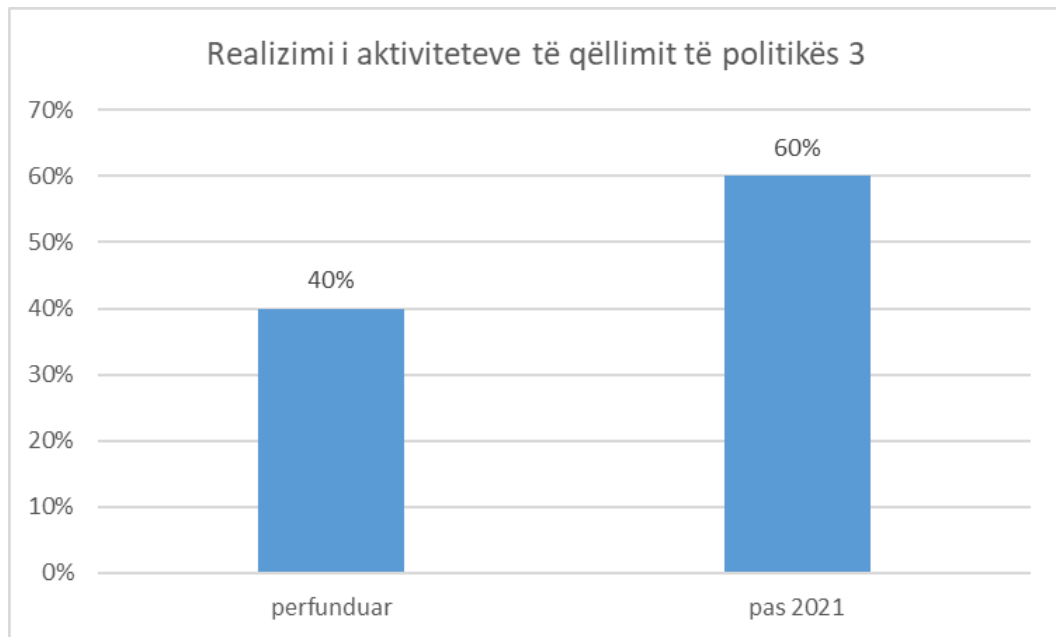


Figure 3 Realizimi i aktiviteteve të qëllimit të politikës 3

Në realizimin e objektivave të qëllimit të politikës së katërt janë parashikuar 15 aktivitete (12%), 11 prej të cilave të realizuara plotësisht dhe 4 të pafilluara akoma siç shihet në grafik.



Figure 4 Realizimi i aktiviteteve të qëllimit të politikës 4

Raporti i plotë i monitorimit gjendet në faqen zyrtare të AKCESK: [https://cesk.gov.al/Publikime/2022/Monitorimi\\_i\\_strategjise\\_sigurise\\_kibernetike\\_2021.pdf](https://cesk.gov.al/Publikime/2022/Monitorimi_i_strategjise_sigurise_kibernetike_2021.pdf)

### 1.2.2 Aktivitete për rritjen e ndërgjegjësimit

Sektori i komunikimit dhe shpërndarjes së informacionit ka marrë pjesë në koordinimin dhe bashkërendimin e punës për realizimin e aktiviteteve në kuadër të projektit të përbashkët me UNICEF Albania “Zhvillimi i mekanizmave të nevojshëm për sigurinë në internet të fëmijëve dhe të rinjve në Shqipëri” gjatë Shkurt – Shtator 2022.

#### **Rezultatet e këtij projekti janë:**

- ✓ Hartimi i 6 dokumentave, në formën e protokollit ndërinstitucional, udhëzues, raport analizues
- ✓ Trajnuar 518 prindër dhe edukatorë në 12 njësi / qytete të Shqipërisë: Babrru, Vorë, Kavajë, Dibër, Klos, Kukës, Has, Laknas, Burrel, Bulqizë, Fushe Arrëz, Pukë, Vau Dejës, Shkodër, Tropojë, Kamëz dhe Paskuqan.
- ✓ Hartuar 1 manual ndërgjegjësimi për prindërit dhe edukatorët, me këshilla për mbrojtjen e fëmijëve në internet, me fokus trafikimin online.

#### **Dokumentat e hartuar janë:**

- Raport për analizimin dhe identifikimin e mekanizmave të raportimit të përmbajtjeve të paligjshme.
- Protokollin ndërinstitucional për bashkëpunimin midis agjencive ligjzbatuese, ofruesve të shërbimit të internetit dhe AKCESK.
- Raport për analizimin dhe identifikimin e hendekut ligjor të mbrojtjes së fëmijëve online nga abuzimi seksual, duke përfshirë rekomandimet e nevojshme.
- Raport për analizimin e funksionaliteteve teknike të Portalit për Bllokimin e Faqeve me Përmbajtje të Paligjshme, së bashku me rekomandimet për përmirësimin e funksionaliteteve me qëllim rritjen e eficiencës.
- Raport për analizimin e iniciativave ekzistuese të Ofruesve të Shërbimit të Internetit për mbrojtjen e fëmijëve në internet.
- Udhëzim për integrimin e Internet Watching Foundation Hash List në shërbimet e Ofruesve të shërbimit të internetit.

Gjithashtu, sektori i komunikimit dhe shpërndarjes së informacionit ka marrë pjesë në koordinimin dhe bashkërendimin e punës për realizimin e aktiviteteve në kuadër të pilotimit të projektit global me International Telecommunication Union “Creating a safe and empowering digital environment for children” për periudhën Janar-Dhjetor 2022.

#### **Rezultatet e këtij projekti janë:**

- ✓ Hartimi i 2 manualeve ndërgjegjësues:
  - Child-friendly manual – i dedikuar për mbrojtjen e fëmijëve në internet
  - Train of Trainers (ToT) Manual – i dedikuar për prindërit, për rritjen e sigurisë së fëmijëve në internet
- ✓ 37 trajnime për fëmijë e të rinj, prindër dhe edukatorë, përfaqësues të industrisë
  - 12 trajnime për fëmijë e të rinj
  - 15 trajnime për prindër dhe edukatorë
  - 10 trajnime për përfaqësues të industrisë

- ✓ 750 pjesëmarrës në trajnime
  - 190 fëmijë e të rinj
  - 460 prindër dhe edukatorë
  - 100 përfaqësues të industrisë
- ✓ 1 mesazh i unifikuar i publikuar në dyqanet fizike dhe mediat sociale të Ofruesve të Shërbimit të Internetit.
- ✓ 1 poster me këshilla nga Udhëzimet e ITU.

## **Aktivitete për rritjen e kapaciteteve**

### **Regional Cyber Camp 19-21 Prill 2021**

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike në bashkëpunim me Geneva Centre for Security Council (DCAF), OSBE, Regional Cooperation Council (RCC), Dhomën Amerikane të Tregtisë në Shqipëri, Shoqatën Shqiptare të Mikrofinancës, One Telecommunications organizuan në datat 19-21 Prill eventin inovativ "Regional Cyber Camp Albania" në ambientet e Hotel Movenpick, Gjiri i Lalzit. Qëllimi i eventit ishte zhvillimi i aftësive praktike për bashkëpunim dhe shkëmbim informacioni midis CSIRT, Policisë së Shtetit dhe institucioneve të tjera rajonale përgjegjëse për sigurinë kibernetike si dhe ngritja e kapaciteteteve të të rinjve mbi sigurinë kibernetike. Përgjatë 3 ditëve të aktivitetit rreth 100 të rinj dhe 50 profesionistë nga Shqipëria, Kosova, Serbia, Bosnjë Hercegovina, Maqedonia e Veriut dhe Mali i Zi thelluan njohuritë e tyre dhe shkëmbyen praktikatat më të mira kombëtare të fushës së sigurisë kibernetike.



### **CyberSec 3.0 22-23 Dhjetor 2022**





Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike organizoi dy ditë rradhazi, me të gjitha Infrastrukturat Kritike të Informacionit të ndara sipas sektorëve, trajnimin e thelluar për "Menaxhimin e incidentit kibernetik", në përmbushje të objektivave të "Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025". Qëllimi i trajnimit është në vazhdim të rritjes së kapaciteteve profesionale të nevojshme për operatorët e infrastrukturave kritike në Shqipëri, si një ndër objektivat kryesore të Autoritetit. Gjithashtu, u organizua stërvitje kibernetike me skenarë të mbështetur në praktikat më të mira.



### 1.2.2 Materiale promovuese

Përgjatë vitit 2022 në zbatim të planit të komunikimit të sektorit u krye realizimi dhe publikimi në rrjetet sociale të Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike i 3 videove promovuese për ndërgjegjësimin e komunitetit për rritjen e nivelit të sigurisë kibernetike, të cilat kanë arritur më shumë se 6000 view në media sociale.

**“Creating a safe and prosperous cyber space for children”**



AKCESK | AUTORITETI KOMBËTAR PËR  
CERTIFIKIMIN ELEKTRONIK  
DHE SIGURINË KIBERNETIKE

Creating a safe and prosperous cyber space for children!

Autoriteti Kombetar per CESK  
27 subscribers

5,155 views 13 Apr 2022

- Video [“Siguria e fëmijëve në internet”](#)
- Video [“Këshilla për prindërit dhe edukatorët për sigurinë e fëmijëve në internet”](#)
- Video [“Udhezime per industrine e mbrojtjes se femijeve ne Internet”](#)

Gjithashtu, periodikisht janë hartuar blog, lajme dhe artikuj, bazuar në analizën e situatës aktuale të ICT dhe sigurisë kibernetike, në kanalet zyrtare të komunikimit në media sociale të Autoritetit.

# 1.2.3 Buletinet e sigurisë kibernetike

## Janar 2022

### Buletini i Lajmeve të Sigurisë Kibernetike

**HAKERËT PO AKSESOJNË LLOGARITË E CEO-VE ME ANË TË APLIKACIONEVË MASHTRUJESË OAUTH**

**DITA E MBROJTJES SË TË DHENAVE**

**KAMERAT E SIGURISË TË LIDHURA ME WIFI MUND TË MANIPULOHEN LEHTË**

**VULNERABILITY SPOTLIGHT**

**DITA E MBROJTJES SË TË DHENAVE**

**SHUMICA E RANSOMWARE JANË TË VETË-INSTALUAR**

**DITA E INTERNETIT TË SIGURT**

**Together for a better internet**

**KONTAKT**  
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039  
Email: info@cesk.gov.al  
Web: www.cesk.gov.al

## Shkurt 2022

### Buletini i Lajmeve të Sigurisë Kibernetike

**SI TË MBROJMË ASETET, INFRASTRUKTURAT DHE IDENTITETIN TONË DIGJITAL**

**DITA NËRKOMBËTARE E GRAVE DHE VAJZAVE NË SHKENCË**

**DITA E INTERNETIT TË SIGURT**

**Together for a better internet**

**KONTAKT**  
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039  
Email: info@cesk.gov.al  
Web: www.cesk.gov.al

## Mars 2022

### Buletini i Lajmeve të Sigurisë Kibernetike

**GJURIMI I AKTIVITETIT KIBERNETIK NË EVROPËN LINDORE**

**PËRDITËSIMI I "PATCH TUESDAY" I MICROSOFT-IT**

**PESË TENDENCA KRYESORE TË SIGURISË KIBERNETIKE PËR 2022**

**MICROSOFT KONFRIMON THYERJEN E SIGURISË NGA GRUPI LAPSUSS**

**KONTAKT**  
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039  
Email: info@cesk.gov.al  
Web: www.cesk.gov.al

## Prill 2022

### Buletini i Lajmeve të Sigurisë Kibernetike

**REGIONAL CYBER CAMP ALBANIA 2022**

**LOG4J- MIJËRA APLIKACIONE JANE ENDE VULNERABEL**

**GOOGLE UPDATE-ON CHROME PËR HERË TË TRETË GJATË 2022**

**KONTAKT**  
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039  
Email: info@cesk.gov.al  
Web: www.cesk.gov.al

## Maj 2022

## Qershor 2022





### 1.3 Sektori i Kontrollit

Në përmbushje të detyrave funksionale, Sektori i Kontrollit gjatë periudhës **Janar- Dhjetor 2022**, ka audituar me metodën (onsite) vajtje në vend, 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 2022, Sektori i Kontrollit ka audituar:

- ⇒ **6** Operatorë të Infrastrukturave Kritike të Informacionit, përshirë sektorët Shëndetësor, Financiar (Bankar, Mikrofinanciar), Energjetik
- ⇒ **5** Operatorë të Infrastrukturave të Rëndësishme të Informacionit, përfshire sektorin Shëndetësor dhe Financiar (Tregu i Sigurimeve)

Gjatë auditave të realizuara pranë operatorëve të infrastrukturave kritike dhe operatoreve të infrastrukturave të rëndësishme të informacionit janë kontrolluar implementimi i masave organizative dhe teknike si më poshtë:

#### **Masat Organizative**

- Politika e sigurisë
- Menaxhimi i riskut
- Siguria organizative
- Kërkesat e sigurisë për palët e treta
- Siguria e burimeve njerëzore dhe aksesit të personave
- Menaxhimi i Aseteve
- Ngjarjet e sigurisë dhe menaxhimit të incidenteve të sigurisë kibernetike
- Menaxhimi i vazhdimësisë së punës
- Menaxhimi i sigurisë së informacionit
- Kontrolli dhe auditimi

#### **Masat Teknike**

- Siguria fizike
- Menaxhimi për autorizimin e aksesit
- Pajisjet kriptografike
- Zbulimi i ngjarjeve të sigurisë kibernetike
- Mjetet e gjurmimit dhe vlerësimit të ngjarjeve të sigurisë kibernetike
- Mbrojtja e integritetit të rrjeteve të komunikimit
- Verifikimi i identitetit të përdoruesve
- Veprimtaria e administratorëve dhe përdoruesve
- Siguria e aplikacioneve
- Siguria e sistemeve industriale

### 1.3.1 Auditimi i Ofruesve të Kualifikuar të Shërbimit të Besuar

Në përmbushje të detyrave funksionale Sektori i Kontrollit gjatë **vitit 2022**, ka mbikëqyrur veprimtarinë e Ofruesit e Kualifikuar të Shërbimit të Besuar (ALEAT), duke inspektuar zyrat e aplikimit për pajisjen me certifikata elektronike të kualifikuara në zbatim të kuadrit ligjor përkatës.

Gjithsej, janë inspektuar **12** Qarqe, si më poshtë:

1. Tiranë
2. Berat
3. Dibër
4. Durrës
5. Elbasan
6. Korçë
7. Fier
8. Gjirokastrë
9. Kukës
10. Lezhë
11. Shkodër
12. Vlorë

Ofruesit e Kualifikuar të Shërbimit të Besuar kanë detyrimin ligjor të raportojnë periodikisht mbi veprimtarinë e tyre pranë AKCESK.

### **OKSHB ALEAT**

Përgjatë periudhës **Janar- Dhjetor 2022**, Aleat ka pajisur me certifikata elektronike të kualifikuara në total **338181** qytetarë në letërnjoftimet ID, si dhe janë shfuqizuar rreth **69370** Certifikata elektronike të kualifikuara.

Që nga lançimi i shërbimit në vitin 2016, deri në Dhjetor 2022, përafërsisht janë kryer rreth 301.330.654 transaksione elektronike të sigurta duke përdorur identifikimin dhe nënshkrimin elektronik.

### **OKSHB AKSHI**

Përgjatë periudhës **Janar-Dhjetor 2022**, OKSHB AKSHI ka lëshuar:

**8499** Certifikata elektronike me nënshkrim elektronik për Administratën Publike

**15943** Certifikata elektronike me nënshkrim elektronik për Subjektet Private

**3512** Certifikata elektronike për sistemin e-receta

**101 599** Certifikata Elektronike për projektin e fiskalizimit për subjektet private production

**1173** Certifikatat elektronike për projektin e fiskalizimit për institucionet shtetërore production

**120** Vula e elektronike për administratën publike

### 1.3.2 Vlerësimi i sigurisë nëpërmjet masave emergjente të sigurisë kibernetike

Spektori i Kontrollit ka kryer vlerësimin e sigurisë nëpërmjet masave emergjente në të gjitha infrastrukturat kritike të informacionit dhe infrastrukturat e rëndësishme të informacionit të miratuara në VKM nr. 553 date 15.07.2020.

Janë vlerësuar në total:

- ⇒ **42** operatore të infrastrukturave kritike të informacionit
- ⇒ **29** operatore të infrastrukturave të rëndësishme të informacionit.

Vlerësimi i sigurisë nëpërmjet masave emergjente të sigurisë u bazua në indikatorët e mëposhtëm:

1. Licencimin e sistemeve kritike/rëndësishme, pajisjet e rrjetit si dhe pajisjet fundore
2. Përdorimin e sistemeve End of Life (EOL)
3. Përdorimin e sistemeve me firmware të vjetër
4. Përdorimin e sistemit qendror të licencuar për menaxhimin e azhurnimeve (patch-eve) të sistemit të operimit
5. Përdorimin e sistemit qendror të licensuar për menaxhimin e azhurnimeve (patch-eve) të Antivirusit
6. Identifikimi dhe përcaktimi i administratorit me të drejta të plota në sistemet kritike/të rëndësishme.
7. Përdorimin e sistemit qendror për monitorimin e vazhdueshëm të rrjetit (Central heuristic traffic analysis)
8. Kryerja e filtrimeve dhe monitorimit të trafikut të rrjetit midis aplikacioneve dhe internetit (Web Application Firewall)
9. Kryerja e analizimeve të lidhjeve në distancë (remote access analysis) të pajisjeve me sistemet/rrjetet kritike/të rëndësishme
10. Kryerja e backup të sistemeve kritike/ të rëndësishme për vazhdimësinë e biznesit

### 1.3.3 Vlerësimi i riskut të sigurisë kibernetike

Përgjatë vitit 2022 është kryer vlerësimi i riskut të sigurisë kibernetike për institucionet e sigurisë dhe mbrojtjes, përkatësisht për:

1. Ministrinë e Mbrojtjes
2. Drejtorinë e Përgjithshme e Policisë Së Shtetit
3. Agjencinë e Mbikëqyrjes Policore
4. Drejtorinë e Sigurimit të Informacionit të Klasifikuar
5. Këshillin e Lartë Gjyqësor
6. Këshillin e Lartë të Prokurorisë
7. Kuvendi
8. Institucioni i Presidentit të Republikës
9. Inspektoratin e Lartë të Deklarimit dhe Kontrollit të Pasurive dhe Konfliktit të Interesave
10. Prokurorinë e Përgjithshme



#### 1.3.4 Hartimi i kuadrit të ri ligjor

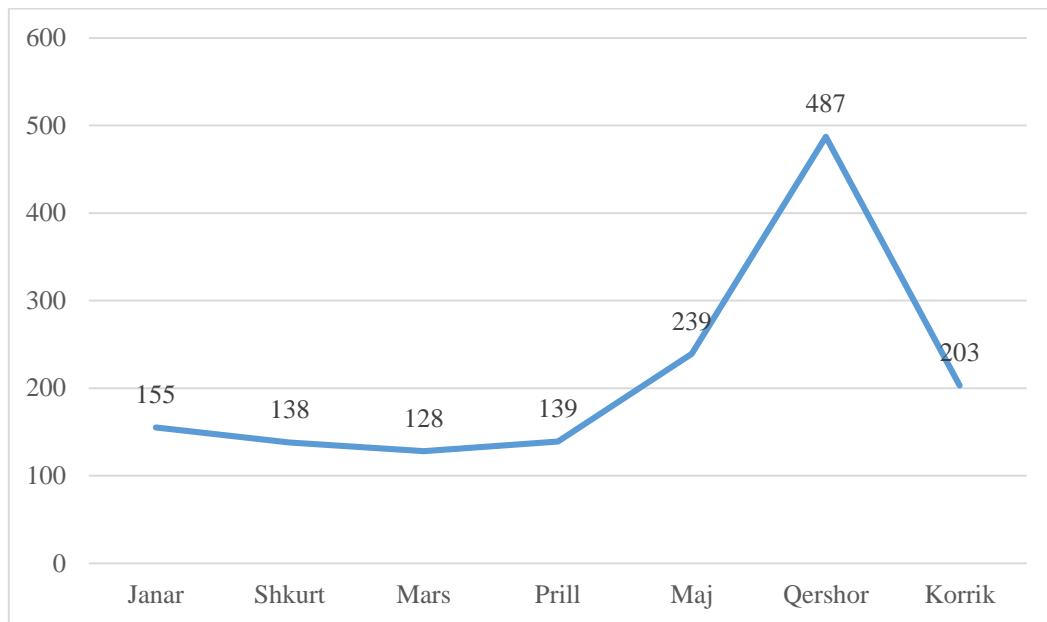
Përgjatë vitit 2022, Sektori i Kontrollit ka dhënë kontribut në draftimin e kuadrit ligjor “Për identifikimin elektronik dhe shërbimet e besuara”, transpozuar nga rregullorja e BE eIDAS 910/2014, si dhe kuadrit ligjor “Për sigurinë kibernetike” transpozuar nga direktiva e BE NIS 1 dhe nis 2.

## 2. Drejtoria e AL-CSIRT

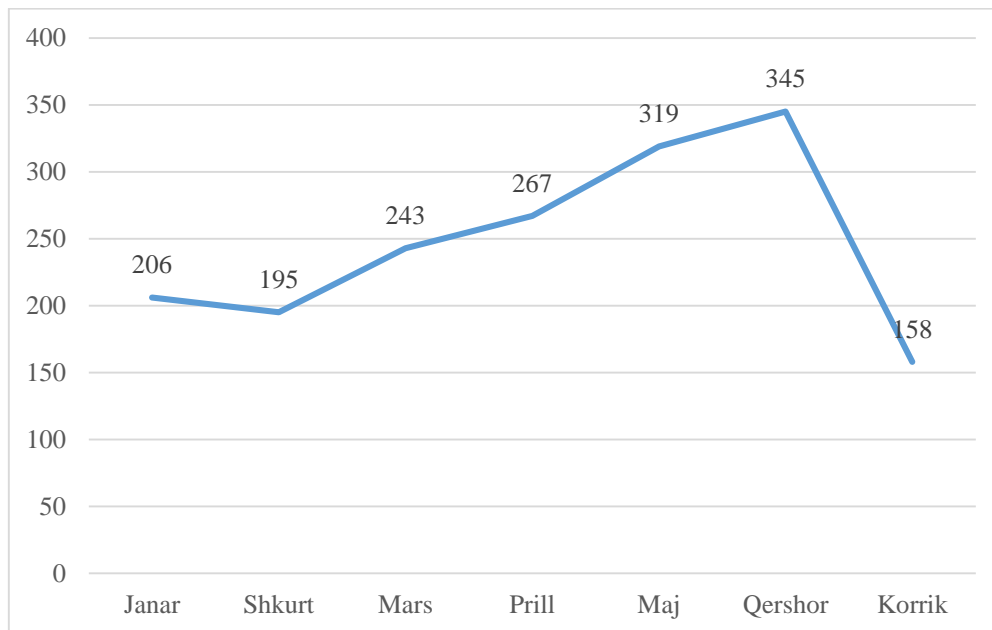
### 2.1 Sektori i monitorimit të incidenteve kibernetike

1. Identifikimi dhe klasifikimi i infrastrukturave kritike dhe të rëndësishme të informacionit në bazë të Ligjit 2/2017 “Për Sigurinë Kibernetike” neni 6, dhe rishikimit të VKM -së nr. 553, date 20.07.2020. Identifikimi dhe klasifikimi është bërë në bazë të sektorëve si më poshtë (Bashkëpunim):
  - Sektori Energjetik: 14 Infrastruktura Kritike të Informacionit dhe 13 Infrastruktura të Rëndësishme të Informacionit
  - Sektori i Transportit: 31 Infrastruktura Kritike të Informacionit dhe 6 Infrastruktura të Rëndësishme të Informacionit
  - Sektori Bankar: 20 Infrastruktura Kritike të Informacionit dhe 52 Infrastruktura të Rëndësishme të Informacionit
  - Sektori Shëndetësor: 17 Infrastruktura Kritike të Informacionit dhe 8 Infrastruktura të Rëndësishme të Informacionit
  - Furnizimi me ujë: 6 Infrastruktura Kritike të Informacionit dhe 44 Infrastruktura të Rëndësishme të Informacionit
  - Infrastruktura Digjitale: 54 Infrastruktura Kritike të Informacionit dhe 25 Infrastruktura të Rëndësishme të Informacionit
2. Në zbatim të VKM-së nr. 141, datë 22.02.2017, AKCESK administron dhe mirëmban sistemin unik on-line, për publikimin e faqeve të internetit 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 2022 ka raportuar në Portalin Online 25 faqe me përmbajtje të paligjshme të cilat janë evidentuar në rrjetet sociale dhe youtube.
3. Monitorimi i disa institucioneve shtetërore dhe Internet Service Provider që operojnë në Shqipëri të cilët gjenerojnë malware me burim (source) Shqipërinë dhe me destinacion shtete të ndryshme, nëpërmjet informacionit që vjen nga Shadow Server. Përpunimi i të dhënave të nxjerra nga ky monitorim si dhe hartimi i raportit. Si më poshtë jepen grafikët përkatës për çdo institucion dhe ISP duke i shprehur me institucion 1 dhe institucion 2, gjithashtu edhe ISP –të me, ISP 1 etj

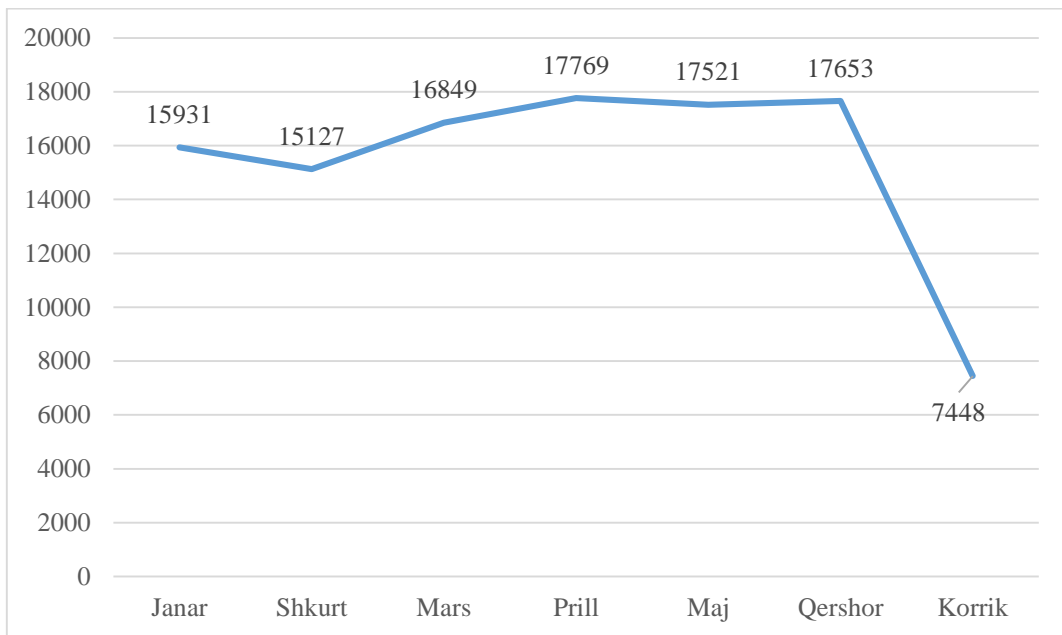
### Institucioni -1



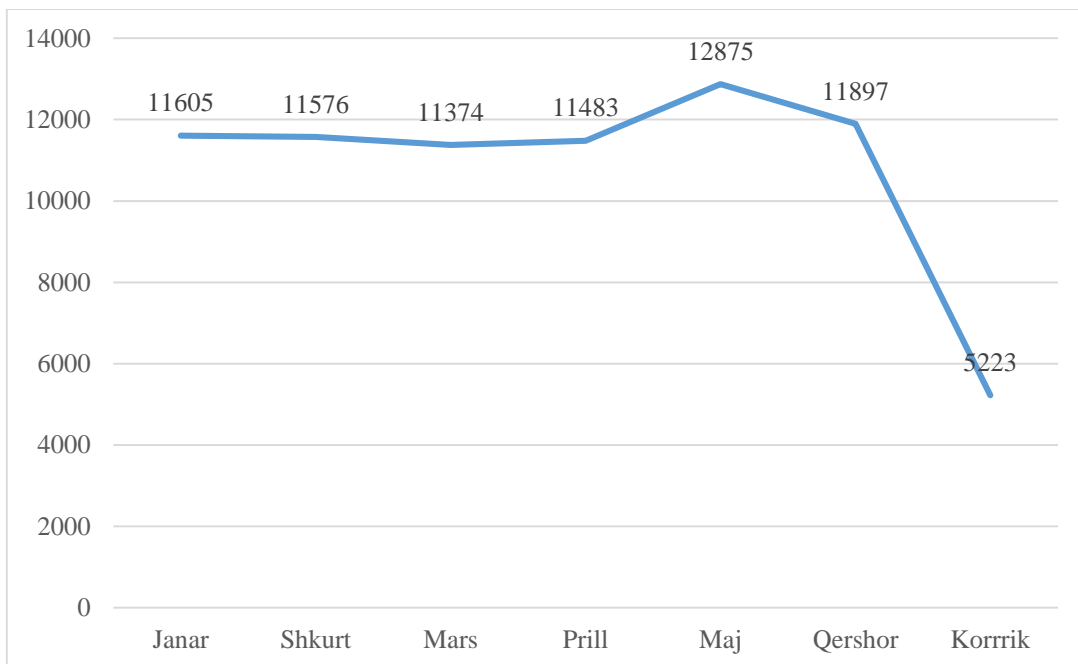
### Institucioni -2



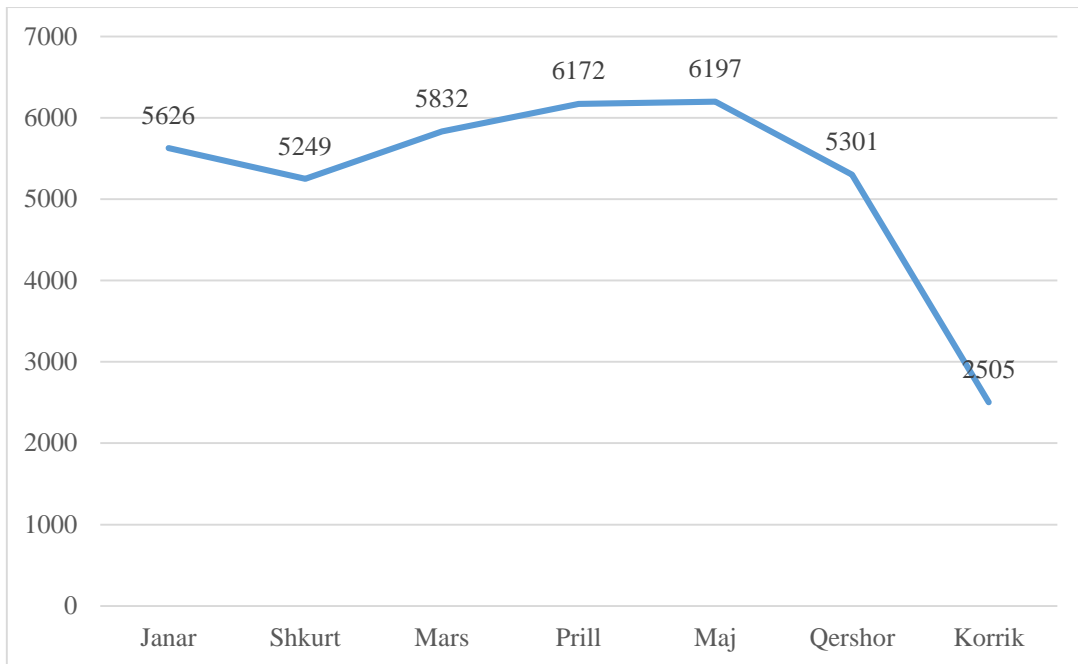
### ISP -1



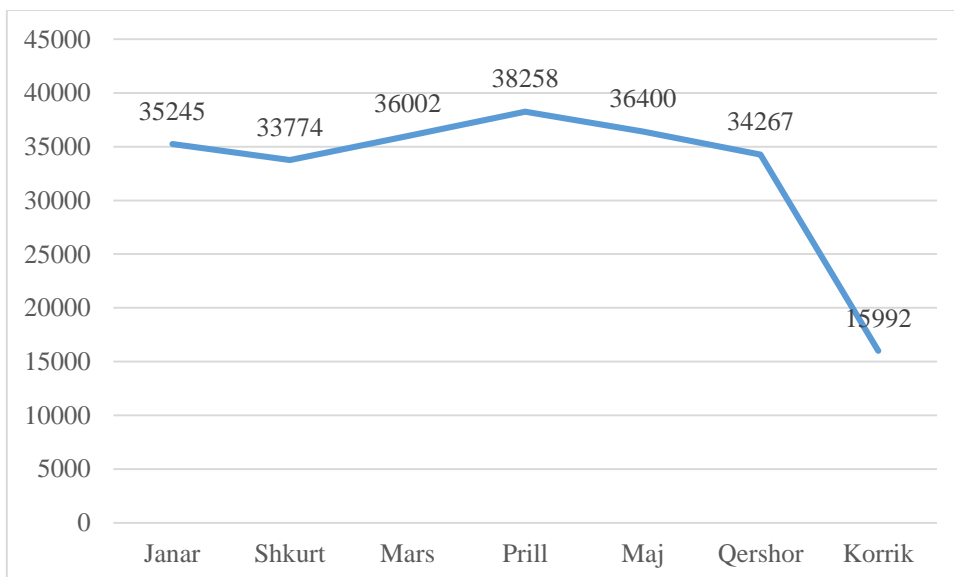
### ISP -2



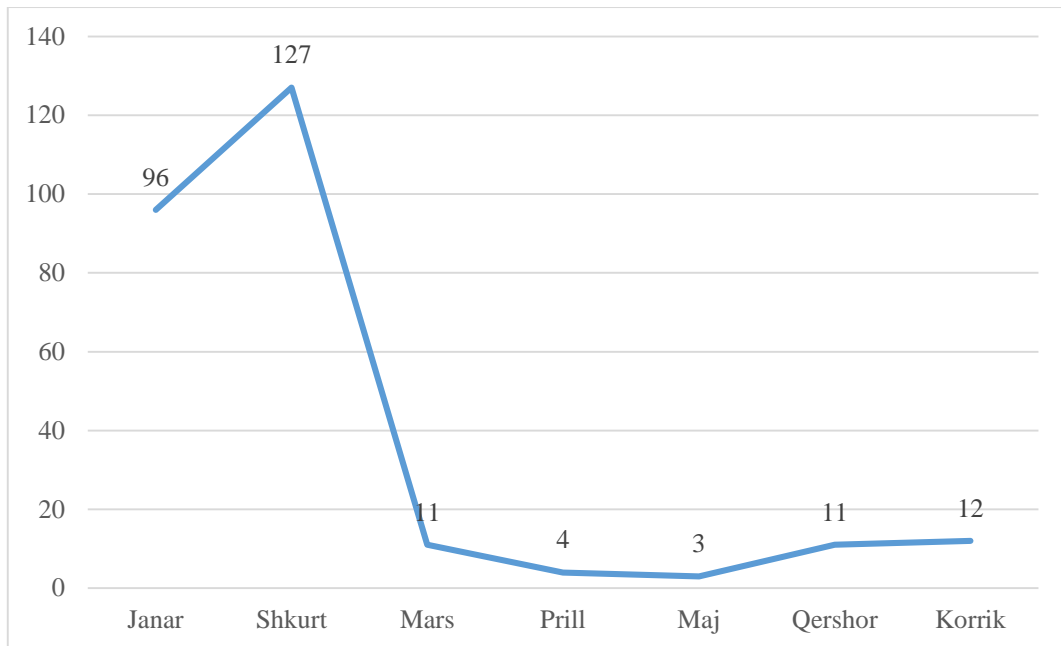
### ISP -3



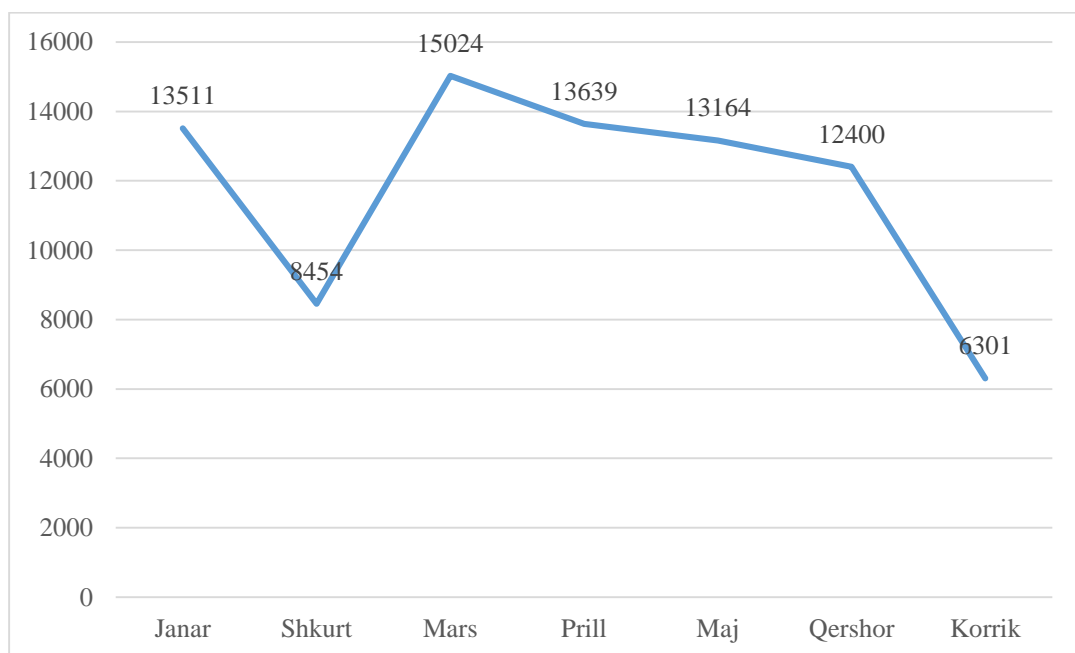
**ISP -4**



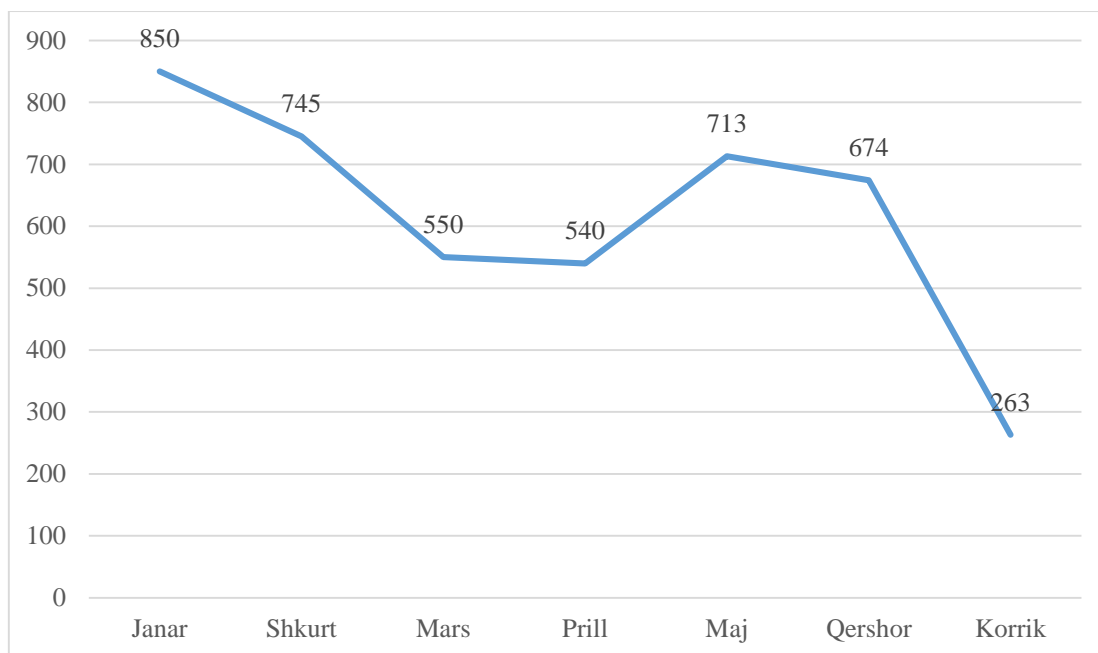
**ISP -5**



**ISP -6**



**ISP -7**



4. Në bashkëpunim draftimin e ligjit “Për Sigurinë Kibernetike”, bazuar në NIS Directive (EU 2016/1148) “Për masat e nivelit të lartë të sigurisë dhe sistemet e informacionit në vendet e BE”.
5. Hartimi i shkresave, raporteve, relacioneve, memo sipas nevojave të institucionit dhe kërkesave të titullarit.

## 2.2 Sektori i menaxhimit të incidenteve kibernetike

- Realizimi i monitorimit të sistemit mbi raportimin dhe menaxhimin e incidenteve kibernetike, në Infrastrukturave Kritike dhe të Rëndësishme të teknologjisë së informacionit.
- Bashkërendimi i punës për zgjidhjen e incidenteve të sigurisë kibernetike me operatorët përgjegjës në fushën e sigurisë kibernetike kombëtare dhe ndërkombëtare.
- Kryerja e kërkimeve të vazhdueshme mbi zhvillimet në fushën e sigurisë kibernetike dhe rekomandon përditësime sigurie në rastin e konstatimeve të vulnerabiliteteve.
- Testimi i Malware të ndryshëm të raportuar ose jo nga OIKI/OIRI duke shfrytëzuar kapacitetet teknike të stafit si dhe Sistemit “Malware Analysis”. Gjithashtu dhe krijimi i raporteve për veprimtarinë e këtyre programeve se bashku me masat për parandalimin e menaxhimin e këtyre aktiviteteve – Periodik.
- Ndihme teknike dhe metodike mbi dekriftimin e informacionit të kompromentuar Policia e shtetit, përmes shkresave.
- Analize pentest per OSHEE.AL, FSHU.AL, OSSH.AL, FTL.AL.

- Analize pentest per UnionBank.
- Raport Akshi incident goxml, cl.exe analizimi i sulmit nga loget e vena ne dispozicion. Eshte bere nje raport i detajuar i sulmit, pavaresisht klasifikimit te tij si Krim Kibernetik.
- Suport per te gjithë Operatoret e infrastrukturave kritike dhe te rendesishme te informacionit rreth qasjes dhe aksesimit te Sistemit te menaxhimit te incidenteve kibernetike. (VPN dhe UsbToken, kur kane patur problematika, jane asistuar remote te gjithë).
- Kerkese AKSHI per mjedise virtuale MISP (platforme per malware sharing).
- Kerkese AKSHI per kapacitete virtuale ARCTIC SECURITY (platforme per threat intelligence).

**Raportet e hedhura ne sistem se fundmi Nga Tetor 2022 - 14 Dhjetor 2022. Raportet jane udhezime, rekomandime dhe kundermasa per incidentet e fundit te ndodhura ne rajon dhe jo vetem:**

- ✚ Perditesimet e fundit mbi ransomware qe targetojne Europen dhe USA, IcedID IOCs dhjetor 5-8 2022, Trickbot IOCs dhjetor 6-11 2022, Cisa 5 new vulnerabilities. [14.12.2022]
- ✚ Akcesk ne bashkepunim me agjensite kombetare ka konstatuar aktivitete malinje nga disa IP te cilat mund te afektojne sistemet e OIKI/OIRI. Bashkangjitur disponohen IOCs dhe rekomandimet perkatese. [13.12.2022]
- ✚ Raport Grupi MuddyWater APT eshte rikthyer me TTP te perditesuar [12.12.2022]
- ✚ Perditesimet e fundit mbi ransomware qe targetojne Europen dhe USA, Ransomware 5-9 dhjetor 2022, Ndikimi i gjere i APT MuddyWater i lidhur me Iranin, Pershkrim informues per sulmet e fundit te periudhes 5-9 dhjetor. [12.12.2022]
- ✚ IP malinje qe shperndajne sulme kibernetike (28 Nentor – 5 Dhjetor 2022). IcedID te njohur si BokBot malware. Njoftim rreth Trickbot malware modular. Ursnif (i njohur si Gozi) malware Trojan Bankar. Renditur IP-te per vendosjen e tyre ne blacklist. [09.12.2022]
- ✚ IP malinje qe shperndajne sulme. 28 Nentor – 5 dhjetor 2022. [09.12.2022]
- ✚ Weekly update 2022-12-02.pdf. Informacione per sulme te ndodhura ne fillim te dhjetorit ne vende te Europes, nga grupi Ragnar Locker Ransomware. [05.12.2022]
- ✚ TLP\_AMBER Ursnif IOCs November 21-27.zip [05.12.2022]
- ✚ Akcesk ndan treguesit ne lidhje me rrjetin e infrastruktures Trickbot i cili eshte nje malware modular i cili per doret per vjedhje informacioni dhe hedhje ransomware. [24.11.2022]

- ✚ IP qe shkaktojne infektimin me ransomware. Tabele me secilen bashkangjitur. Udhezues qe perfshin teknika dhe procedura (TTP) si dhe tregues te kompromisit (IOCs) per te ndihmuar organizatat te mbrohen nga sulmet ransomware. [18.11.2022]
- ✚ Perditesimi javor i qendres se mbrojtjes Lituanese mbi sulmet ransomware te ndodhura javen e pare dhe te dyte te nentorit ne Ukraine dhe Bullgari. Rekomandime te renditura me qellim parandalimin e sulmeve te tilla dhe aktiviteteteve te tjera keqdashese. (Weekly update 2022-11-18.pdf) [18.11.2022]
- ✚ Hakerat kineze synojne agjencite qeveritare dhe organet e mbrojtjes.pdf [16.11.2022]
- ✚ Ransomware (Ragnar Locker) qe prek palet e aviacionit.pdf [08.11.2022]
- ✚ Weekly update 2022-10-28.pdf. DdoS dhe ransomware te ndodhura javen e shkuar ne Ukraine dhe Poloni (kryesisht ne sektorin financiar) dhe Izrael(Knesset Website). [31.10.2022]
- ✚ FBI, CISA, HHS kane publikuar disa informacione keshilluese dhe udhezuese te Sigurise kibernetike mbi Ekipin Daixin grup krimi kibernetike qe synon ne menyre aktive (hedhje te ransomware dhe operacioneve te vjedhjes se te dhenave) bizneset amerikane, sektorin e kujdesit shendetesor dhe shendetit publik. [26.10.2022]
- ✚ Perditesimi i Qendres Lituanese te Mbrojtjes Kibernetike mbi sulmet Ransomware dhe DdoS. Weekly update 2022-10-21.pdf [26.10.2022]

### 3. Sektori i financës dhe shërbimeve mbështetëse

Për Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike buxheti i alokuar për vitin 2022 është 57,952 mijë lekë nga të cilat 53,952 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	30,122,400	24,382,994	81%
601	4,590,525	4,011,919	87%
602	18,876,000	5,728,198	30%
606	364,000	273,458	75%
231	4,000,000	702,000	18%
Shuma	57,952,925	35,098,569	



*Fondi i Pagave dhe Sigurimeve Shoqërore (zërat 600+601)* Shumat e alokuara për paga dhe sigurime shoqërore për vitin 2022 janë përkatësisht 30,122,400 lekë për artikullin 600 dhe 4,590,525 lekë për artikullin 601. Dhe realizimi është përkatësisht 24,382,994 lekë për artikullin 600 dhe 4,011,919 lekë për artikullin 601.

*Fondi për shpenzime në mallra dhe shërbime (zëri 602)* Shuma e alokuar për vitin 2022 për shpenzime operative është 18,876,000 lekë. Dhe realizimi për këtë artikull është 5,728,198 lekë.

*Fondi i Veçantë (zëri 606)* Shuma e alokuar për vitin 2022 për shpenzime për ndihma në fatkeqësi është 364,000 lekë. Dhe realizimi për këtë artikull është 273,548 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 702,000 lekë.

Në muajin Tetor të vitit 2022 marrëdhëniet e punës të punonjësve të Autoritetit ndryshuan nga nëpunës civilë në marrëdhënie me Kod Pune.

Gjatë vitit 2022 kemi bërë rekrutime të reja duke e shtuar numrin e stafit me 4 persona.