**A logo with a crown and a letter

Description automatically generated**

**СТРАТЕГИЈА**

**ЗА БОРБУ ПРОТИВ САЈБЕР КРИМИНАЛИТЕТА У РЕПУБЛИЦИ СРПСКОЈ**

**ЗА ПЕРИОД ОД 2025. ДО 2031. ГОДИНЕ**

**Стратешка платформа**

**НАЦРТ**

1. Јануар 2025. године

**САДРЖАЈ**

[**Скраћенице** 3](#_Toc186463701)

[**УВОД** 4](#_Toc186463702)

[**1. СТРАТЕШКА ПЛАТФОРМА** 6](#_Toc186463703)

[**1.1. СИТУАЦИОНА АНАЛИЗА** 6](#_Toc186463704)

[**Сајбер криминалитет у Републици Српској** 6](#_Toc186463705)

Међународни – правни оквир.....................................................................................................6

Законски оквир сајбер криминалитета у Републици Српској...................................................9

1.1.1. Процјена остварења претходне Стратегије за борбу против сајбер криминалитета у Републици Српској.........................................................................................11

Акциони план за борбу против сајбер криминалитета у Републици Српској 2023 – 2024. година.....................................................................................................................................11

Акциони план за заштиту дјеце од сексуалног злостављања и искориштавања у Републици Српској 2023 – 2024. година...............................................................................13

Извјештај о реализацији активности за Акциони план за борбу против сајбер криминалитета у Републици Српској за период јануар 2020 – децембар 2022. године..16

Извјештај о реализацији активности за Акциони план за заштиту дјеце од порнографије у Републици Српској 2020–2022. за период јануар 2022 – децембар 2022. године.........17

[**1.1.2.Aнализа сајбер криминалитета у Републици Српској** 20](#_Toc186463706)

[**1.1.3.Стање и трендови сајбер криминалитета у Европи и свијету** 28](#_Toc186463707)

[**1.1.4.Институционални механизми борбе против сајбер криминалитет**](#_Toc186463708) 40

[**1.2.** **SWOT АНАЛИЗА И СТРАТЕШКО ФОКУСИРАЊЕ** 43](#_Toc186463709)

[**1.2.1.SWOT анализа** 43](#_Toc186463710)

[**1.2.2.Стратешки фокуси** 45](#_Toc186463711)

[**1.3.Стратешка визија** 46](#_Toc186463712)

[**1.3.1.Стратешки циљеви** 46](#_Toc186463713)

# **Скраћенице**

|  |  |
| --- | --- |
| **ГС** | Генерални секретаријат |
| **МУП** | Министарство унутрашњих послова |
| **МП** | Министарство правде |
| **МФ** | Министарство финансија |
| **МНРВО** | Министарство за научнотехнолошки развој и високо образовање |
| **МЗСЗ** | Министарство здравља и социјалне заштите |
| **МПК** | Министарство просвјете и културу |
| **МПОС** | Министарство породице, омладине и спорта |
| **МПП** | Министарство привреде и предузетништва |
| **МЕИМС** | Министарство за европске интеграције и међународну сарадњу |
| **РЈТ РС** | Републичко јавно тужилаштво Републике Српске |
| **ЦЕСТ РС** | Центар за едукацију судија и тужилаца Републике Српске |
| **АИКТ** | Агенција за информационо – комуникационе технологије |
| **АДУ** | Агенција за државну управу |
| **ЕУ** | Европска Унија |

# **УВОД**

Стратегија за борбу против сајбер криминалитета у Републици Српској за период од 2025. до 2031. године, (у даљем тексту: Стратегија) представља стратешки документ, који утврђује краткорочне, средњорочне и дугорочне циљеве и приоритете борбе против сајбер криминалитета у Републици Српској. Стратегија је израђена у складу са Законом о стратешком планирању Републике Српске[[1]](#footnote-1), који уређује поступак доношења Стратегије, њен обухват и надлежности за њену израду и доношење.

Стратегија представља основ за израду спроведбених докумената и планирање буџетских средстава из буџета Републике Српске за реализовање активности из поменутих докумената.

Потреба за израдом Стратегије настала је из чињенице да је временски период важења постојећег стратешког документа у области сајбер криминалитета (Стратегија за борбу против сајбер криминалитета у Републици Српској за период 2020-2024. године) истекао, као и због све веће учесталости и сложености сајбер криминалитета, што захтијева свеобухватан и усклађен приступ у његовом спречавању и сузбијању, те прилагођавање новим технолошким изазовима и безбједносним ризицима.

Такође, претходни стратешки документ није био ни методолошки усклађен са Законом о стратешком планирању и управљању развојем у Републици Српској из 2021. године, из ког разлога је опредјељење било да се приступи изради стратешког документа који ће представљати основу за проактивно и систематско рјешавање изазова у области борбе против сајбер криминалитета, с циљем унапређења правног оквира, јачања институционалних капацитета, те успостављања ефикасних механизама за превенцију, откривање и расвјетљавање кривичних дјела у дигиталном окружењу.

Рјешењем министра унутрашњих послова Републике Српске (број: С/М-3-052-3691/24 од 8.11.2024. године) именована је Радна група за израду Стратегије за борбу против сајбер криминалитета у Републици Српској за период 2025-2031. године (у даљњем тексту: Радна група) са задатком да припреми приједлог стратешког документа користећи методолошки поступак који је дефинисан Законом о стратешком планирању и управљању развојем у Републици Српској и Уредбом о стратешким документима у Републици Српској.

Сам процес израде Стратегије је спроведен у складу са основним начелима стратешког планирања, Законом и Уредбом о стратешким документима у Републици Српској[[2]](#footnote-2) (у даљњем тексту Уредба) и одвијао се у сљедећим фазама:

1) израда стратешке платформе,

2) одређивање приоритета и мјера,

3) идентификација кључних стратешких пројеката,

4) утврђивање унутрашње и међусобне усклађености стратешког документа,

5) израда оквирног финансијског плана за спровођење стратешког документа,

6) израда оквира за спровођење, праћење, извјештавање и вредновање стратешког документа,

7) спровођење процеса консултација о стратешком документу.

Као резултат прве фазе у изради стратешког документа, припремљена је стратешка платформа која обухвата ситуациону анализу сачињену ради утврђивања постојећег стања, која је укључила сагледавање стања у области сајбер криминалитета у Републици Српској али и Европи и Свијету, реализацију активности из претходне Стратегије за борбу против сајбер криминалитета на период од 2020. до 2024. године, као и сагледавање изазова и потенцијала за унапређење борбе против сајбер криминалитета. На основу ситуационе анализе извршено је стратешко фокусирање и сачињен је приједлог визије, стратешких циљева и индикатора за праћење напретка у остваривању стратешких циљева. На Нацрт стратешке платформе су спроведене јавне консултације и Нацрт стратешке платформе је дискутован у широком партиципативном процесу, уз учешће свих заинтересованих субјеката (институције јавне управе, организације цивилног друштва, представници академске заједнице, привреде и међународних организација). Нацрт стратешке платформе био је доступан за достављање коментара јавности на интернет презентацији Министарства унутрашњих послова Републике Српске.

У сљедећим фазама, сачињен je приједлог приоритета, мјера и кључних стратешких пројеката, укључујући и приједлоге индикатора за праћење успјеха у њиховом спровођењу. Након тога, припремљени су приједлози осталих дијелова Стратегије: опис унутрашње и међусобне усклађености Стратегије, оквирни финансијски план за њено спровођење, оквир за спровођење, праћење, извјештавање и вредновање стратегије и прилози.

У том контексту треба напоменути да је документ Стратегије усклађен са интервенцијама у овој oбласти на европском нивоу гдје је и Европска унија донијела Стратегију за јачање борбе против сајбер криминалитета и Акциони план за спровођење Стратегије у којима се као основни циљеви наводе подстицање држава да у своје законодавство уграде Будимпештанску конвенцију, подизање стандарда у специјализацији полиције, судства, тужилаштва, подстицање размјене информација међу државама и сл. као и са циљевима одрживог развоја у Босне и Херцеговине[[3]](#footnote-3), документима релевантним за процес европских интеграција и другим међународно преузетим обавезама, као и са низом актуелних секторских стратегија у Републици Српској.

На Нацрт стратегије су спроведене широке јавне консултације са свим заинтересованим субјектима након чега ће документ бити упућен у процедуру усвајања.

# **1. СТРАТЕШКА ПЛАТФОРМА**

## **1.1. СИТУАЦИОНА АНАЛИЗА**

### **Сајбер криминалитет у Републици Српској**

Ефикасна борба против сајбер криминалитета у Републици Српској захтијева добро утемељен и свеобухватан правни оквир који ће омогућити превенцију, откривање, истрагу и санкционисање сајбер криминалитета. Овај оквир се ослања на постојеће националне законе и подзаконске акте, али истовремено узима у обзир међународне стандарде и инструменте, који су кључни за хармонизацију и јачање глобалне сарадње.

Убрзани развој дигиталних технологија отворио је нове могућности за развој друштва, али и изазове у виду сајбер криминалитета. Како би се осигурала ефикасна борба против овог облика криминалитета, нормативни оквир представља један од основних стубова заштите, превенције и реаговања. Његов значај огледа се у препознавању сајбер криминалитета као специфичног облика криминалитета, успостављању правних основа за истрагу и санкционисање, усклађености са међународним стандардима, јачању институционалних капацитета и превенцији и едукацији.

#### **Међународни – правни оквир**

Конвенција о високотехнолошком криминалитету, позната као Будимпештанска конвенција, донесена 23. новембра 2001. године (на снази од јула 2004. године), један је од најважнијих међународних докумената који се бави компјутерским криминалитетом. Будимпештанска конвенција спада у круг оквирних конвенција, што значи да њене одредбе нису директно примјењиве, већ је неопходно да их државе реализују кроз своје национално законодавство. Будимпештанска конвенција бави се материјалноправним, процесноправним и организационим питањима борбе против компјутерског криминалитета.

Конвенција прави разлику између четири различите врсте кривичних дјела:

1. Дјела против повјерљивости, интегритета и доступности компјутерских података и система – њих чине незаконит приступ, пресретање, уплитање у податке или системе, кориштење уређаја (производња, продаја, увоз, дистрибуција), програма, лозинке,
2. Дјела у вези са компјутерима – код којих су фалсификовање и крађе најтипичнији облици напада,
3. Дјела у вези са садржајима – дјечија порнографија је најчешћи садржај који се појављује у овој групи кривичних дјела, обухватајући посједовање, дистрибуцију, трансмисију, чување или чињење доступним и расположивим ових материјала, њихова производња ради дистрибуције и обрада у компјутерском систему или на носиоцу података и
4. Дјела у вези са кршењем ауторских и сродних права – обухватају репродуковање и дистрибуцију неауторизованих примјерака дјела компјутерским системима.

Такође, битно је споменути и Протокол уз Конвенцију о високотехнолошком криминалитету који се односи на дјела расистичке и ксенофобне природе почињених помоћу рачунарских система. Протокол предвиђа да државе пропишу као посебна кривична дјела ширење расног и ксенофобног материјала путем рачунара, пријетње и увреде мотивисане расизмом и ксенофобијом извршене путем рачунара, порицање злочина геноцида и других злочина против човјечности извршених путем рачунара.

Други додатни протокол на Будимпештанску конвенцију који је од суштинског значаја за савремену борбу против сајбер криминалитета. Усвојен је 2021. године у Стразбуру и представља значајан корак у јачању међународне сарадње у борби против сајбер криминалитета. Циљ овог протокола је да побољша могућности за откривање, прибављање и размјену електронских доказа, који су кључни за истраге и гоњење сајбер криминалитета. С обзиром на то да је сајбер криминалитета често транснационалне природе, овај протокол пружа јасне правне механизме за ефикаснију међународну сарадњу.

Кључни аспекти Другог додатног протокола:

1. Унапређење међународне сарадње које се огледа у

* Директној сарадњи са интернет провајдерима (Протокол омогућава органима власти у једној земљи да директно комуницирају са провајдерима у другој земљи ради добијања података)
* Стандардизацији процедура (уводи јасне и стандардизоване процедуре за подношење захтјева и обраду информација)

2. Нови механизми за прибављање електронских доказа

Други протокол уводи иновативне алате за прибављање електронских доказа, који су од виталног значаја за истраге сајбер криминала:

* Омогућава правосудним органима да директно приступе основним подацима о претплатницима (нпр. име и адреса) код провајдера у страној јурисдикцији.
* Привремено чување података (Протокол омогућава захтјев за чување података који могу бити од значаја за истрагу, чиме се спречава њихово брисање или уништење)
* Механизам за хитне случајеве (Протокол успоставља брзу процедуру за прибављање информација у ситуацијама које захтијевају хитно дјеловање (нпр. спречавање терористичких аката или заштита жртава))

3.Заштита људских права и података

* Усаглашеност са међународним стандардима: Протокол је усклађен са Европском конвенцијом о људским правима и другим међународним инструментима за заштиту људских права.
* Заштита података: Пружа јасне оквире за обраду и пренос података, уз осигурање њихове заштите.

4.Јачање правних основа за сарадњу (подстиче закључивање билатералних или мултилатералних споразума који могу додатно олакшати сарадњу између држава)

5.Транспарентност и надзор: Успоставља механизме који обезбјеђују транспарентност и надзор над активностима у оквиру сарадње.

Такође је битно споменути и УН конвенцију о сајбер криминалитету[[4]](#footnote-4) која се бави материјалноправним, процесноправним и организационим питањима борбе против компјутерског криминалитета. Сврхе ове конвенције су:

(а) промовисање и јачање мјера за ефикасније и дјелотворније спречавање и борбу против сајбер криминалитета;

(б) Промовисање, олакшавање и јачање међународне сарадње у спречавању и борби против сајбер криминалитета; и

(в) Промовисање, олакшавање и подржавање техничке помоћи и изградња капацитета за превенцију и борбу против сајбер криминала, посебно у корист земаља у развоју.

Kонвенција Савета Европе о заштити дјеце од сексуалног искоришћавања и сексуалног злостављања (тзв. Ланзарот конвенција – Савјет Европе 2007. година), између осталог, дефинише кривична дјела у вези са дјечијом порнографијом, као посебним обликом сексуалне експлоатације и злоупотребе дјеце. Поред тога, ова конвенција препоручује да свака страна потписница усваја мјере неопходне да би се осигурало да лица, јединице или службе задужене за истрагу буду специјализоване у области борбе против сексуалног искоришћавања и сексуалног злостављања дјеце или да та лица буду обучена у те сврхе (тзв. принцип специјалности). Она, такође, прописује да ће свака земља потписница предузети све неопходне законодавне или друге мјере да би омогућила јединицама истражних служби да идентификују жртве кривичних дјела, посебно помоћу анализе порнографског материјала, као што су фотографије и аудио-визуелни записи емитовани или стављени на располагање помоћу информационо -комуникационе технологије.

Одлуком Савјета Европске уније о сузбијању дјечје порнографије на интернету 2000/375/JHA, препоручено је да, ако је потребно, мјере за промовисање ефикасне истраге и кривичног прогона за кривична дјела на том подручју, могу бити и установљавање посебних јединица при органима надлежним за извршавање закона која имају потребна стручна знања и средства да би ефикасно поступали на основу информација о могућој производњи, обради, дистрибуцији и посједовању дјечје порнографије. Овом одлуком је препоручено да државе чланице установе властити систем надзора сузбијања производње, обраде, посједовања и дистрибуције материјала с дјечјом порнографијом.

Директива Европског парламента о борби против сексуалне злоупотребе и искориштавања дјеце и дјечије порнографије 2011/93ЕУ препоручује државама чланицама да предузму неопходне мјере да омогуће истражним јединицама или службама да идентификују жртве кривичних дјела (сексуална злоупотреба, сексуална експлоатација, дјечја порнографија и тзв. grooming), посебно анализом материјала дјечје порнографије, као што су фотографије и аудио-видео записи емитовани или стављени на располагање помоћу информационе и комуникационе технологије.

Директива 2013/40/ЕУ Европског парламента и Савјета ЕУ о нападима на информационе системе и замјени Оквирне одлуке Савјета 2005/222/JHA се односи на нападе усмјерене против информационих система. Њен циљ је да приближи кривичним законодавствима земаља чланица ЕУ област напада на информационе системе, успостављањем минималних правила који се односе на дефиницију кривичних дјела и одговарајућих кривичноправних санкција, као и унапређивање сарадње између надлежних органа који укључују припаднике полиције и других специјализованих агенција за спровођење закона чланица ЕУ, као и надлежних специјализованих агенција и тијела Европске уније, као што су EUROJUST, EUROPOL или његов Европски центар за борбу против сајбер криминала (ЕC 3), као и укључивање у рад Европске агенције за безбједност мрежа и података (ЕNISА).

Схватајући огромну опасност од сајбер криминалитета и Европска унија је донијела Стратегију за јачање борбе против сајбер криминалитета и Акциони план за спровођење Стратегије у којима се као основни циљеви наводе подстицање држава да у своје законодавство уграде Будимпештанску конвенцију, подизање стандарда у специјализацији полиције, судства, тужилаштва, подстицање размјене информација међу државама и сл.

#### **Законски оквир сајбер криминалитета у Републици Српској**

Најзначајнији дио правног оквира у Републици Српској за борбу против сајбер криминалитета чине сљедећи закони:

1. Кривични законик Републике Српске (Службени гласник Републике Српске број: 73/23)
2. Закон о кривичном поступку Републике Српске (Службени гласник Републике Српске број: 53/2012, 91/2017, 66/2018 i 15/2021)
3. Закон о посебном регистру лица правоснажно осуђених за кривична дјела сексуалне злоупотребе и искориштавања дјеце (Службени гласник Републике Српске број: 28/23)

Кривични законик Републике Српске у Глави XXXII прописује сљедећа кривична дјела против безбједности компјутерских података:

1. Оштећење компјутерских података и програма;
2. Компјутерска саботажа;
3. Израда и уношење компјутерских вируса;
4. Компјутерска превара;
5. Неовлаштен приступ заштићеном компјутеру, компјутерској мрежи, телекомуникационој мрежи и електронској обради података;
6. Спречавање и ограничавање приступа јавној компјутерској мрежи; и
7. Неовлаштено кориштење компјутера или компјутерске мреже.

Поред кривичних дјела против безбједности компјутерских података Кривични законик Републике Српске у Глави XV прописује кривична дјела сексуалног злостављања и искоришћавања дјетета. У поменутој глави Кривичног законика из аспекта спречавања сајбер криминалитета посебно је битна инкриминација сљедећих кривичних дјела:

1. Искориштавање дјеце за порнографију;
2. Искориштавање дјеце за порнографске представе;
3. Упознавање дјеце с порнографијом; и
4. Искориштавање компјутерске мреже или комуникације другим техничким средствима за извршење кривичних дјела сексуалног злостављања или искориштавања дјетета.

Поред наведених, постоје и остала кривична дјела која се доводе у везу са високотехнолошким криминалитетом као што су: Прогањање, Угрожавање сигурности, Повреда тајности писама или других пошиљки, Неовлаштено прислушкивање и тонско снимање, Неовлаштено фотографисање, Неовлаштено објављивање и приказивање туђег списа, портрета и снимка, Неовлашћено коришћене личних података, Полна уцјена, Полно узнемиравање, Злоупотреба фотографије и видео-записа полно експлицитног садржаја, Повреда приватности дјетета, Клевета, Превара, Изнуда, Уцјена, Прање новца, Јавно подстицање на терористичку активност, Фалсификовање кредитних картица и картица за безготовинско плаћање, иЈавно изазивање и подстицање насиља и мржње.

Анализом поменутих кривичних дјела видљив је један свеобухватан законски приступ који инкриминише данас фреквентна дјела из области сајбер криминалитета.

Када је у питању сајбер криминалитет битно је споменути да Закон о кривичном поступку Републике Српске представља оквир за дјеловање полицијских и правосудних органа приликом процесуирања дјела сајбер криминалитета. Закон о кривичном поступку прописује правила која се примjењују на криминалистичке истраге, укључујући начине прикупљања и обраде дигиталних доказа, што је основно за дjеловање органа за спровођење закона у случајевима компјутерског криминалитета. Такође, компјутески криминалитет је глобални феномен, па се овим законом такође омогућава и правни оквир за сарадњу са другим земљама, када је ријеч о изручењу, међународној правној помоћи и размјенама доказа у циљу процесуирања кривичних дјела који имају прекогранични карактер.

* + 1. **Процјена остварења претходне Стратегије за борбу против сајбер криминалитета у Републици Српској**

Република Српска има Стратегију за борбу против сајбер криминалитета у Републици Српској која се односи за период од 2020. до 2024. године те три акциона плана који су произашли из стратегије и то: Акциони план за борбу против сајбер криминалитета у Републици Српској за период од 2023. до 2024. године, Акциони план за заштиту дјеце од сексуалног злостављања и искориштавања дјеце у Републици Српској на период од 2023. до 2024. године и Акциони план за дигиталну форензику за период од 2023-2024. године (у периоду од 2020-2022. године такође три акциона плана и то: Акциони план за борбу против сајбер криминалитета у Републици Српској за период од 2020. до 2022. године, Акциони план за заштиту дјеце од порнографије у Републици Српској за период од 2020. до 2022. године и Акциони план за дигиталну форензику за период од 2020. до 2022. године)

Стратегија за борбу против сајбер криминалитета у Републици Српској на период од 2020. до 2024. године дефинише пет стратешких циљева:

1) Подизање свијести и едукација заједнице;

2) Унапријеђен законодавни оквир за борбу против сајбер криминалитета у Републици Српској;

3) Унапријеђени капацитети републичких органа (људски и материјално технички) за борбу против сајбер криминалитета;

4) Унапријеђена сарадња између свих органа који учествују против сајбер криминалитета (јавни и приватни сектор);

5) Унапријеђена међународна сарадња у циљу ефикасне размјене информација и заједничких истрага.

С тим вези, извршен је преглед реализације акционих планова произашлих из Стратегије.

**Акциони план за борбу против сајбер криминалитета у Републици Српској 2023 – 2024. година**

Како је већ наведено, Стратегија за борбу против сајбер криминалитета у Републици Српској на период од 2020. до 2024. године дефинише пет стратешких циљева, али како је ступио на снагу нови Закон о стратешком планирању и управљању развојем у Републици Српској и Уредба о спроведбеним документима у Републици Српској („Службени гласник Републике Српске“ број: 8/21) којим се, уређује систем стратешког планирања, приступило се изради Акционог плана за борбу против сајбер криминалитета у Републици Српској 2023 – 2024. година, у складу са новом методологијом. У том смислу, стратешки циљеви дефинисани стратегијом су прилагођени у акционом плану како би се адекватно одредили кључни стратешки пројекти, приоритети, мјере и активности. Овим није промијењена концепција Стратегије, а сви циљеви из Стратегије обухваћени су кључним стратешким пројектима и приоритетима.

Акциони план за борбу против сајбер криминалитета у Републици Српској за период од 2023. до 2024. године дефинише два стратешка циља:

1. Унапређење капацитета за превентивно дјеловање у области борбе против сајбер криминалитета у Републици Српској и
2. Унапређење капацитета за репресивно дјеловање у области борбе против сајбер криминалитета у Републици Српској.

За сваки од наведених стратешких циљева дефинисани су приоритети, мјере, кључни стратешки пројекти, активности кроз које се циљ реализује, индикатори успјешности реализације активности, носиоци активности као и потребни финансијски ресурси.

Кратак опис акционог плана (укупна финансијска вриједност акционог плана, процентуални преглед извора финансирања, кључни стратешки пројекти, итд .)

Укупан буџет потребан за реализовање приоритета, мјера и активности ~~а~~кционог плана за период 2023. године и 2024. године износи 147.000 КМ, а гледано по годинама за 2023. годину износи 50.000 КМ док за 2024. годину износи 97.000 КМ.

Кључни стратешки пројекти Акционог плана су:

1. Спроводити обуке за запослене у институцијама, носиоцима спречавања сајбер криминалитета, са циљем подизања свијести запослених o oпасностима од сајбер криминалитета и
2. Остваривати сарадњу и вршити размјену информација са институцијама за спровођење закона у другим државама и међународним организацијама за чију реализацију је планирано.

Средства за реализацију Акционог плана планирана су из буџета Владе Републике Српске и предвиђена Годишњим и Средњорочним планом Министарства унутрашњих послова Републике Српске. Очекујемо да се током имплементације Акционог плана обезбиједе и додатна финансијска средства кроз одређене пројекте и донације, која током израде Акционог плана није било могуће прецизирати.

|  |  |
| --- | --- |
| **Циљеви:** | **Процјена остварења:** |
| **ЦИЉ 1:** Унапређење капацитета за превентивно дјеловање у области борбе против сајбер криминалитета у Републици Српској | Број реализованих мјера на информисању и едуковању заједнице у борби против сајбер криминалитета  Дјелимично реализована мјера са 13 активности од којих је 12 реализовано  Број реализованих мјера на унапређењу законодавног оквира  Дјелимично реализована мјера са 5 активности од којих су 4 реализоване  Број реализованих мјера на унапређењу капацитета републичких органа за борбу против сајбер криминалитета    Дјелимично реализована мјера са 8 активности од којих је 7 реализовано  Број реализованих мјера на унапређењу сарадње између свих органа који учествују у борби против сајбер криминалитета  У потпуности реализована мјера са 4 активности од којих су све реализоване  **Укупно су предвиђене 4 мјере са 30 активности од којих je реализованo 27 активности.** |
| **ЦИЉ 2:** Унапређење капацитета у области репресивног дјеловања на сузбијању сајбер криминалитета | Број предузетих мјера на унапређењу међународне сарадње у области сајбер криминалитета.  У потпуности реализована мјера са 6 активности од којих су све реализоване.  Број предузетих мјера на унапређењу међуинституционалне сарадње у Републици Српској у области сајбер криминалитета.  У потпуности реализована мјера са 4 активности од којих су све реализоване.  Број предузетих мјера на унапређењу међуинституционалне сарадње са институцијама у БиХ.  У потпуности реализована мјера са 3 активности од којих су све реализоване.  **Укупно 3 мјере/ 13 активности од којих је 13 реализовано.** |

Табела 1. Приказ реализације активности Акционог плана за борбу против сајбер криминалитета у Републици Српској 2023-2024. годину

**Акциони план за заштиту дјеце од сексуалног злостављања и искориштавања у Републици Српској 2023 – 2024. година**

Влада Републике Српске рјешењем број: 04/1-012-2-2561/22 од 21.07.2022 именовала је Радну групу за израду Акционог плана за заштиту дјеце од порнографије у Републици Српској 2023 -2024. година. Чланови Радне групе су предложили да се назив Акциони план за заштиту дјеце од порнографије у Републици Српској мијења у назив Акциони план за зашиту дјеце од сексуалног злостављања и искориштавања у Републици Српској, јер се термин дјечија порнографија сматра термином који иде у прилог извршиоцима предметних кривичних дјела предметних кривичних дјела. Односно, термин порнографија представља нешто што је сексуално стимулативно а дијете, одраслој особи са исправном перцепцијом, не смије бити сексуално стимулативно, те се с тим у вези, сматра да се свака сексуална активност усмјерена ка дјеци мора сматрати насиљем, злостављањем или искориштавањем. Термин искориштавање и злостављање дјеце адекватније описује противзаконите радње усмјерене ка дјеци. С тога је назив Акционог плана за заштиту дјеце од сексуалног злостављања и искориштавања у Републици Српској једногласно прихваћен.

С обзиром да је ступио на снагу Закон о стратешком планирању и управљању развојем у Републици Српској („Службени гласник Републике Српске“ број: 63/21) и Уредба о спроведбеним документима у Републици Српској („Службени гласник Републике Српске“ број: 8/21) којим се уређује систем стратешког планирања, приступило се изради Акционог плана за заштиту дјеце од сексуалног злостављања и искориштавања у Републици Српској 2023 – 2024. година, у складу са новом методологијом. У том смислу, како би се адекватно одредили кључни стратешки пројекти, приоритети, мјере и активности, стратешки циљеви дефинисани Стратегијом су прилагођени у акционом плану чиме није промијењена концепција Стратегије, а сви циљеви из Стратегије обухваћени су кључним стратешким пројектима и приоритетима.

Акциони план за заштиту дјеце од сексуалног злостављања и искориштавања у Републици Српској 2023 -2024. година приоритете, мјере и активности је груписао у два стратешка циља:

1. Унапређење капацитета за превентивно дјеловање у области борбе против сајбер криминалитета у Републици Српској и
2. Унапређење капацитета за репресивно дјеловање у области борбе против сајбер криминалитета у Републици Српској.

За сваки од наведених стратешких циљева дефинисани су приоритети, мјере, кључни стратешки пројекти, активности кроз које се циљ реализује, индикатори успјешности реализације активности, носиоци активности као и потребни финансијски ресурси.

Укупан буџет потребан за реализацију приоритета, мјера и активности из акционог плана за период 2023. године и 2024. године износе 147.000 КМ, а гледано по годинама за 2023. годину износи 50.000 КМ док за 2024. годину износи 97.000 КМ.

Кључни стратешки пројекти Акционог плана су:

1. Спроводити обуке за запослене у институцијама, носиоцима спречавања криминалитета који се односи на сексуално злостављање и искориштавање дјеце, са циљем подизања свијести запослених o oпасностима од сексуалне злоупотребе и искориштавања дјеце у дигиталном окружењу и
2. Остваривати сарадњу и вршити размјену информација са институцијама за спровођење закона у другим државама и међународним организацијама за чију реализацију је планирано.

Средства за реализацију Акционог плана планирана су из буџета Владе Републике Српске и предвиђена Годишњим и Средњорочним планом Министарства унутрашњих послова Републике Српске. Напомињемо, да су иста средства планирана и за Акциони план за борбу против сајбер криминалитета у оквиру мјере *Унаприједити борбу против свих видова криминалитета, нарочито организованог криминала, корупције и тероризма*, Средњорочног плана Министарства унутрашњих послова, а кроз активност *Унапређени капацитети за одговор на сајбер напад и откривање и расвјетљавање кривичних дјела сајбер криминалитета.* Очекујемо да се током имплементације Акционог плана обезбиједе и додатна финансијска средства кроз одређене пројекте и донације, која током израде Акционог плана није било могуће прецизирати.

|  |  |
| --- | --- |
| **Циљеви:** | **Процјена остварења:** |
| **ЦИЉ 1:** Унапређење капацитета за превентивно дјеловање у области борбе против сајбер криминалитета у Републици Српској | Број реализованих мјера на информисању и едуковању заједнице у области заштите дјеце од сексуалног злостављања и искориштавања у дигиталном окружењу.  У потпуности реализована мјера са 8 активности.  Број реализованих мјера на унапређењу законодавног оквира.  Дјелимично реализована мјера са 7 активности од којих је 5 реализовано.  Број реализованих мјера на унапређењу капацитета републичких органа у области заштите дјеце од сексуалног злостављања и искориштавања у дигиталном окружењу.  Дјелимично реализована мјера са 7 активности од којих је 5 реализовано.  Број реализованих мјера на унапређењу сарадње између свих органа који учествују у области заштите дјеце од сексуалног злостављања и искориштавања у дигиталном окружењу.  Дјелимично реализована мјера са 4 активности од којих су 3 реализоване.  **Укупно предвиђене 4 мјере са 26 активности од којих је реализована 21 мјера.** |
| **ЦИЉ 2:** Унапређење капацитета у области репресивног дјеловања на сузбијању сајбер криминалитета | Број предузетих мјера на унапређењу међународне сарадње у области сексуалног злостављања и искориштавања дјеце у дигиталном окружењу.  У потпуности реализована мјера са 5 активности.  Број предузетих мјера на унапређењу међуинституционалне сарадње у Републици Српској у области сексуалног злостављања и искориштавања дјеце у дигиталном окружењу.  У потпуности реализована мјера са 2 активности.  Број предузетих мјера на унапређењу међуинституционалне сарадње са институцијама у БиХ у области сексуалног злостављања и искориштавања дјеце у дигиталном окружењу.  У потпуности реализована мјера са 2 активности.  **Укупно предвиђене 3 мјере са 9 активности од којих су све реализоване.** |

Табела 2. Приказ реализације активности Акционог плана за заштиту дјеце од сексуалног злостављања и искориштавања у дигиталном окружењу у Републици Српској 2023-2024. годину

**Извјештај о реализацији активности за Акциони план за борбу против сајбер криминалитета у Републици Српској за период јануар 2020 – децембар 2022. године.**

Извјештај о реализацији Акционог плана за борбу против сајбер криминалитета у Републици Српској 2020-2022. (у даљњем тексту: Акциони план) представља збир извјештаја носилаца конкретних активности из Акционог плана. Министарство унутрашњих послова Републике Српске је као координатор, прикупило, објединило, систематизовало и обрадило извјештаје носилаца активности, те припремило Извјештај о реализацији Акционог плана, који доставља на усвајање Влади Републике Српске. Саставни дио Извјештаја је табеларни преглед реализованих активности у којем су за сваку од активности наведене конкретне мјере и радње које су реализоване у извјештајном периоду.

Реализација пет стратешких циљева у Акционом плану планирана је кроз 34 активности. Планирани временски оквир за реализовање највећег броја активности је – „континуирано“ (односно, до истека Акционог плана), тако да се реализовање истих наставља и у наредном периоду. Од укупног броја активности, током извјештајног периода, реализовано је 30 активности, што представља 88,2%, а четири активности или 11,76% није реализовано. Преглед реализације броја активности по појединим стратешким циљевима приказан је у табели.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Стратешки циљ** | **Укупно активности** | **Реализација** | | | **Напомена** |
| **Реализовано** | **Није доспјело** | **Није реализовано** |
| Стратешки циљ 1 | 11 | 10 | - | 1 |  |
| Стратешки циљ 2 | 6 | 5 | - | 1 |  |
| Стратешки циљ 3 | 7 | 6 | - | 1 |  |
| Стратешки циљ 4 | 4 | 3 | - | 1 |  |
| Стратешки циљ 5 | 6 | 6 | - | - |  |
| **УКУПНО АКЦИОНИ ПЛАН** | **34** | **30** | **-** | **4** |  |

*Табела 3. Приказ реализације Акционог плана за борбу против сајбер криминалитета у Републици Српској – број реализованих активности током 2022. године*

***Стратешки циљ 1.* Подизање свијести и едукација заједнице.** Реализација овог стратешког циља планирана је кроз 11 активности. Будући да се ради о подизању свијести јавности, едукацији корисника, обиљежавању значајних датума, сарадњи са медијима и финансијским институцијама, односно активностима које се спроводе континуирано и временски оквир за све ове активности је - „континуирано“. Десет активности је током 2022. године реализовано у већем дијелу или у потпуности. Једна планирана активност „Јачање сарадње са финансијским институцијама и спровођење кампања информисања о опасностима од сајбер криминалитета за клијенте банака и слично“ – није реализована.

***Стратешки циљ 2.* Унапријеђен законодавни оквир за борбу против сајбер криминалитета у Републици Српској.** Реализација овог стратешког циља планирана је кроз шест активности. Током 2022. године реализовано је пет активности а једна активност која је планирана током 2022. године – измјена и допуна Закона о кривичном поступку није реализована.

***Стратешки циљ 3.* Унапријеђени капацитети републичких органа (људски и материјално технички) за борбу против сајбер криминалитета.** Реализација овог стратешког циља планирана је кроз седам активности. Будући да се ради о едукацији службеника републичких органа и институција, набавци опреме и усклађивању процедура, односно активностима које се спроводе континуирано и временски оквир за све ове активности је - „континуирано“. Шест активности је током извјештајног периода реализовано у цјелости или у већем обиму. Једна планирана активност „Техничкиопремити институције за провођење закона потребнопм опремом и софтвером за борбу против сајбер криминалитета“ није реализована у извјештајном периоду.

***Стратешки циљ 4.* Унапријеђена сарадња између свих органа који учествују у борби против сајбер криминалитета (јавни и приватни сектор).** Реализација овог стратешког циља планирана је кроз четири активности. У извјештајном периоду три активности су реализоване. Једна планирана активност која се односи на јачање сарадње са представницима приватног сектора ради унапређења спречавања сајбер криминалитета – није реализована.

***Стратешки циљ 5.* Унапријеђена међународна сарадња у циљу ефикасне размјене информација и заједничких истрага.** Реализација овог стратешког циља планирана је кроз шест активности. Како се ради о унапређењу међународне сарадње, односно активностима које се спроводе континуирано и временски оквир за све ове активности је - „континуирано“. Свих шест активности је током извјештајног периода реализовано кроз већи број мјера.

**Извјештај о реализацији активности за Акциони план за заштиту дјеце од порнографије у Републици Српској 2020–2022. за период јануар 2022 – децембар 2022. године**

Извјештај о реализацији Акционог плана за заштиту дјеце од порнографије у Републици Српској 2020-2022. представља збир извјештаја носилаца конкретних активности из Акционог плана. Министарство унутрашњих послова Републике Српске је као координатор прикупило, објединило, систематизовало и обрадило извјештаје носилаца активности, те припремило Извјештај о реализацији активности Акционог плана, који је достављен Влади Републике Српске на усвајање. Саставни дио Извјештаја је табеларни преглед реализације активности у којем су за сваку од активности наведене конкретне мјере и радње које су реализоване у извјештајном периоду.

Реализација пет стратешких циљева у Акционом плану планирана је кроз 27 активности. Планирани временски оквир за реализовање највећег броја активности је – „континуирано“ (односно, до истека Акционог плана), тако да се реализовање истих наставља и у наредном периоду (до краја 2024. године). Преглед реализације броја активности по појединим стратешким циљевима приказан је у табели.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Стратешки циљ** | **Укупно активности** | **Реализација** | | | | **Напомена** |
| **Реализовано** | **У току** | **Није доспјело** | **Није реализовано** |
| Стратешки циљ 1 | 7 | 7 | - | - | - |  |
| Стратешки циљ 2 | 6 | 4 | 1 | - | 1 |  |
| Стратешки циљ 3 | 7 | 6 | - | - | 1 |  |
| Стратешки циљ 4 | 3 | 3 | - | - | - |  |
| Стратешки циљ 5 | 4 | 4 | - | - | - |  |
| **УКУПНО АКЦИОНИ ПЛАН** | **27** | **24** | **1** | **-** | **2** |  |

*Табела 4. Приказ реализације активности Акционог плана за заштиту дјеце од порнографије у Републици Српској – током 2022. године*

Од укупног броја активности, током извјештајног периода, реализовано је у цјелини или већим дијелом укупно 24 активности што представља 88,9%. У току је реализација за једну активност (3.7%), а нису реализоване двије активности (7,4%).

***Стратешки циљ 1.* Подизање свијести и едукација заједнице.** Реализација овог стратешког циља планирана је кроз седам активности. Будући да се ради о подизању свијести јавности, едукацији корисника, обиљежавању значајних датума, сарадњи са медијима и финансијским институцијама, односно активностима које се спроводе континуирано и временски оквир за све ове активности је - „континуирано“. Свих седам активности је реализовано у већем обиму током извјештајног периода.

***Стратешки циљ 2.* Унапријеђен законодавни оквир за борбу против дјечије порнографије у Републици Српској.** Реализација овог стратешког циља планирана је кроз шест активности. Током извјештајног периода 4 активности су реализоване у већем обиму, а започела је реализација још једне од активности. Једна планирана активности везана за развијање, односно измјене и допуне Закона о кривичном поступку у овој области, није реализована.

***Стратешки циљ 3.* Унапријеђени капацитети републичких органа (људски и материјално технички) за борбу против дјечије порнографије.** Реализација овог стратешког циља планирана је кроз седам активности. Како се ради о едукацији службеника републичких органа и институција, набавци опреме и усклађивању процедура, односно активностима које се спроводе континуирано и временски оквир за све ове активности је - „континуирано“. Пет активности су током извјештајног периода реализоване у већем дијелу или у потпуности. Једна активност није реализована која се односи на набавку опреме институција за провођење закона.

***Стратешки циљ 4.* Унапријеђена сарадња између свих органа који учествују против дјечије порнографије (јавни и приватни сектор).** Реализација овог стратешког циља планирана је кроз три активности. Све три активности су реализоване.

***Стратешки циљ 5.* Унапријеђена међународна сарадња у циљу ефикасне размјене информација и заједничких истрага.** Реализација овог стратешког циља планирана је кроз четири активности. Како се ради о унапређењу међународне сарадње, односно активностима које се спроводе континуирано и временски оквир за све ове активности је - „континуирано“. Све активности су током извјештајног периода реализоване у већем дијелу или у потпуности.

## **Aнализа сајбер криминалитета у Републици Српској**

Сајбер криминалитет у Републици Српској биљежи значајан раст последњих година, усљед повећане дигитализације и доступности технологије. У овом дијелу се приказују најважнији подаци и трендови засновани на званичним извjештајима МУП-а РС за период од 2019. од 2024. године, када је у питању сајбер криминалитет.

За анализу сајбер криминалитета у Републици Српској узети су статистички подаци Министарства унутрашњих послова Републике Српске а који кроз графички приказ илуструју број и структуру кривичних дјела.



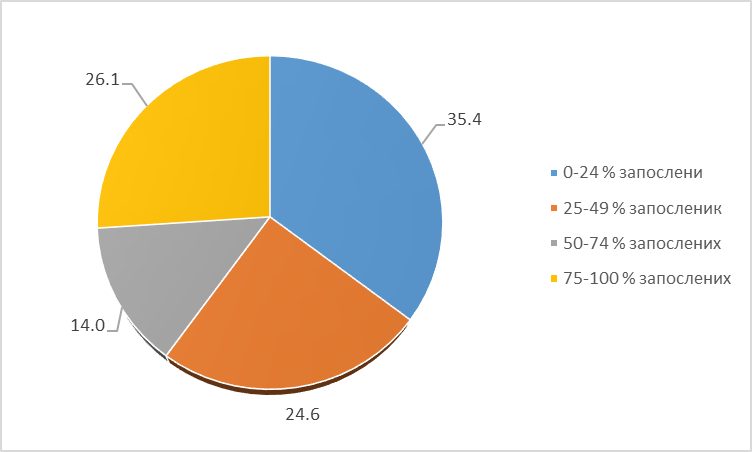
Графикон број 1. Упоредни приказ броја кривичних дјела сајбер криминалитета у периоду 2019-2024. године

Могуће је констатовати нагли пораст броја кривичних дјела у односу између 2019. и 2020. године, након чега је примијетан континуитет и благи пораст из године у годину. (Графикон број 1).

Овај пораст сразмјеран је порасту броја корисника информационих технологија на подручју Републике Српске гдје је присутан општи тренд повећања коришћења и примјене ИКТ у свим сегментима друштвеног и привредног развоја.

Повећана примјена и коришћење ИКТ са собом, осим бенефита, доноси и опасности због чега је неопходно радити на подизању свијести о ризицима сајбер криминалитета али и мјерама самозаштите.

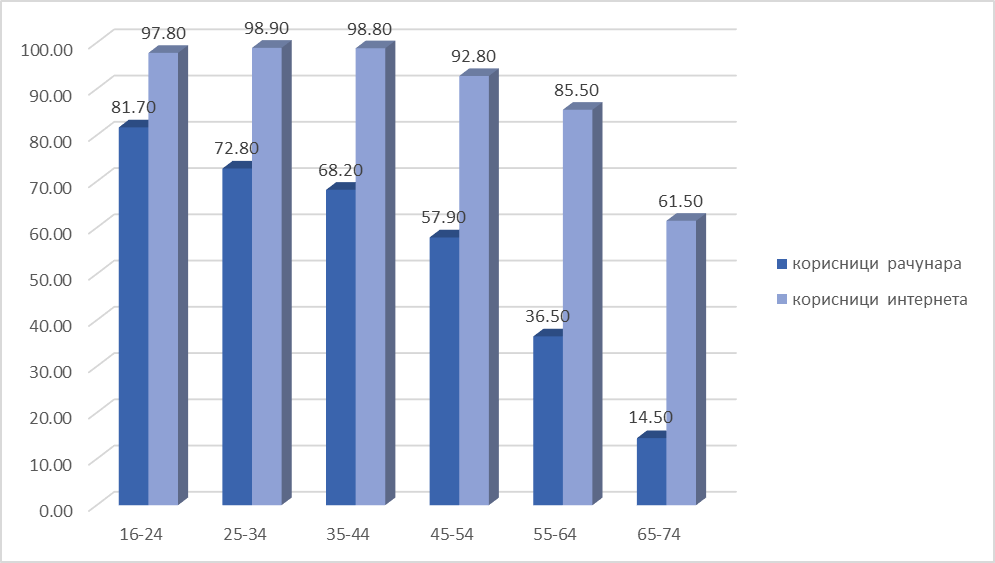
Резултати истраживања о информационо-комуникационим технологијама у предузећима, спроведеног у 2023. години, показују да сва предузећа имају приступ интернету. У сљедећем графикону дат је приказ процента запослених који користе интернет у пословне сврхе.



Графикон број 2.- Предузећа са процентом запослених лица која користе интернет за пословне потребе, 2023. године

Извор: Републички завод за статистику РС

Према истом извору приступ интернету посједује 84,8% домаћинстава. Анализа заступљености интернет конекције у домаћинствима према типу насеља показала је да у градском подручју интернет прикључак посједује 89,1% домаћинстава, а 81,9% домаћинстава у насељима осталог типа. Евидентно је такође да су млади најчешће корисници интернета при чему проценат корисника старосне доби од 16-24 године износи високих 97,8 %.



Графикон број 3.- Корисници рачунара и интернета по старосним групама, 2023. године

Карактеристика кривичних дјела у области сајбер криминалитета је да у значајном броју случајева није могуће одмах квалификовати кривично дјело те је, с тим у вези, изузетно значајан податак о броју активности у области високотехнолошког криминалитета гдје је приказ достављених извјештаја надлежним тужилаштвима о догађајима за које се према тренутно расположивим информацијама није могуће одредити да ли представљају кривично дјело или не, чиме се број предмета високотехнолошког криминалитета у великој мјери повећава. (Графикон број 4)



Графикон број 4. Упоредни приказ броја активности у вези кривичних дјела сајбер криминалитета у периоду 2019-2024. године

Материјална штета проузрокована извршењем кривичних дјела у области сајбер криминалитета је готово у константном порасту и креће се од неколико стотина хиљада па до преко три милиона КМ у претходне двије године. (Графикон број 5)



Графикон број 5. Упоредни приказ износа материјалне штете проузроковане извршењем кривичних дјела сајбер криминалитета у периоду 2019-2024. године

Министарство унутрашњих послова Републике Српске у континуитету спроводи криминалистичке обраде које за циљ имају откривање и доказивање кривичних дјела и извршилаца а усмјерене су на различите врсте криминалних активности. Тако је, Министарство унутрашњих послова Републике Српске у периоду од 2020. године па до мјесеца новембра 2024. године реализовало сљедеће криминалистичке обраде (КО):

* КО кодног назива „Форум“ - заведена са циљем спречавања и сузбијања кривичних дјела која врше лица која путем интернета посјећују мјеста за неовлаштену куповину форумског типа, путем којих врше куповину, продају, као и посредовање у куповини и продаји кредитних картица, опојних дрога, оружја, лијекова као и других роба и услуга. KO је међународног карактера и спроводи се у сарадњи са институцијама за спровођење закона СР Њемачке.
* КО кодног назива „Систем“ - заведена са циљем спречавања и сузбијања кривичних дјела која се односе на искориштавање дјеце за порнографију. КО је међународног карактера.
* КО кодног назива „Плагијат“ - заведена са циљем откривања и доказивања кривичних дјела из области заштите ауторских права. КО је међународног карактера и спроводи се у сарадњи са EUROPOL-om и надлежним институцијама у иностранству.
* КО кодног назива „Seacatch“ - заведена са циљем откривања и доказивања кривичних дјела која се односе на израду и уношење компјутерских вируса са циљем извршавања преваре и уцјене. КО је међународног карактера и спроводи се у сарадњи са надлежним институцијама Велике Британије.
* КО кодног назива „Goldfish RS“ - заведена са циљем предузимања низа активности на откривању и доказивању кривичних дјелаиз области компијутерског криминалитета а која се односе на кривично дјело неовлаштен приступ заштићеном компјутеру, компјутерсој мрежи, телекомуникационој мрежи и електронској обради података. КО je међународног карактера и спроводи са у сарадњи са INTERPOL-om.
* КО кодног назива „Kарика“ - заведена са циљем откривања и доказивања кривичних дјела сексуалног злостављања и искориштавања дјеце. КО је међународног карактера и спроводи се у сарадњи са надлежним институцијама Републике Србије, Републике Хрватске и Републике Црне Горе.
* КО кодног назива „Мрежа“ - заведена са циљем откривања и доказивања кривичних дјела превара и компјутерска превара. КО је локалног карактера и спроводи се у сарадњи са ОЈТ у Добоју и организационим једицама МУП-а на регији.
* КО кодног назива „Вектор 1“- заведена са циљем откривања и доказивања кривичних дјела превара, изнуда и прање новца. КО је локалног карактера и спроводи се у сарадњи са ОЈТ у Требињу и организационим једицама МУП-а на регији.
* КО кодног назива „Пандора“ - заведена са циљем откривања и доказивања кривичних дјела из области заштите неовлаштене трговине културним добрима путем интернета. КО је међународног карактера и спроводи се у сарадњи са INTERPOL-oм и надлежним институцијама за спровођење закона у иностранству.
* КО кодног назива „Вектор“ - заведена са циљем откривања и доказивања кривичних дјела превара, изнуда и прање новца. КО је локалног карактера и спроводи се у сарадњи са ОЈТ у Требињу и организационим једицама МУП-а на регији.
* КО кодног назива „Инстикт“ - заведена са циљем откривања и доказивања кривичних дјела сексуалног злостављања и искориштавања дјеце. КО је локалног карактера и спроводи се у сарадњи Управе криминалистичке полиције и Полицијске управе Приједор.
* КО кодног назива „Идентитет“ - заведена са циљем откривања и доказивања кривичних дјела неовлашћеног коришћења личних података. КО је локалног карактера и спроводи се у сарадњи Управе криминалистичке полиције и надлежним Полицијским управама на регији.
* КО кодног назива „Скрипта“ - заведена са циљем откривања и доказивања кривичних дјела прање новца и неовлаштен приступ заштићеном компјутеру, компјутерској мрежи, телекомуникационој мрежи и електронској обради података. КО је локалног карактера и спроводи се у сарадњи са ОЈТ у Бањалуци и организационим јединицама МУП-а на регији.
* КО кодног назива „Линк“ - заведена са циљем откривања и доказивања кривичних дјела компјутерска превара, прање новца и удруживање ради вршења кривичних дјела. КО је локалног карактера и спроводи се у сарадњи са ФУП-ом.
* КО кодног назива „Купа“ - заведена са циљем откривања и доказивања кривичних дјела израда и уношење компјутерских вируса и изнуда. КО је локалног карактера и спроводи се у сарадњи са ОЈТ у Бањалуци.
* КО кодног назива „First Light“ - заведена са циљем откривања и доказивања кривичних дјела компјутерска превара. КО је међународног карактера и спроводи се у сарадњи са INTEROPOL-om и другим организационим јединицама МУП-а.
* КО кодног назива „Тикет“ - заведена са циљем откривања и доказивања кривичних дјела превара и прање новца, као и других кривичних дјела која су везана за лажне дојаве о намјештеним спортским мечевима. КО је међународног карактера и спроводи се у сарадњи са INTERPOL-om и надлежним институцијама за спровођење закона у БиХ и иностранству.
* КО кодног назива „Виза“ - заведена са циљем откривања и доказивања кривичних дјела неовлаштено кориштење личних података и прање новца. КО је међународног карактера и спроводи се у сарадњи са INTERPOL-om и надлежним институцијама за спровођење закона у БиХ и иностранству.
* КО кодног назива „Типс“ - заведена са циљем откривања и доказивања кривичних дјела превара, изнуда и прање новца. КО је међународног карактера и спроводи се у сарадњи са INTERPOL-om, ПУ Источно Сарајево и уз координацију ОЈТ у Источном Сарајеву.
* КО кодног назива „Мозаик 2023“ - заведедена са циљем откривања и доказивања кривичних дјела искориштавање дјеце за порнографију. КО је међународног карактера и спроводи се у сарадњи са EUROPOL-om, Републиком Србијом, Републиком Словенијом, Републиком Хрватском и Републиком Сјеверном Македонијом.
* КО кодног назива „Ласер“ - заведедена са циљем откривања и доказивања кривичних дјела сексуалног злостављања и искориштавања дјеце. КО је локалног карактера и спроводи се у сарадњи са ПУ Бања Лука.
* КО кодног назива „Монеро“ - заведена са циљем откривања и доказивања кривичних дјела превара, изнуда и прање новца. КО је међународног карактера и спроводи се у сарадњи са INTERPOL-om, EUROPOL-om, полицијским агенцијама земаља региона и ПУ Фоча.
* КО кодног назива „Cumberland RS“ - заведена са циљем откривања и доказивања кривичних дјела сексуалног злостављања и искориштавања дјеце. КО је међународног карактера и спроводи се у сарадњи са EUROPOL-om и другим организационим јединицама МУП-а Републике Српске.

Анализом предметних криминалистичких обрада може се констатовати да је Министарство унутрашњих послова Републике Српске акценат ставило на сљедеће облике криминалитета:

* кривична дјела из области безбједности компјутерских података, гдје посебно истичемо рансомвер, односно кривична дјела Неовлаштени приступ заштићеном компјутеру, компјутерској мрежи, телекомуникационој мрежи и електронској обрaди података, Компјутерска саботажа, Спречавање и ограничавање приступа јавној компјутерској мрежи, Израда и уношење компјутерских вируса и слично;
* кривична дјела сексуалног злостављања и искориштавања дјеце у дигиталном окружењу, гдје се у 2024. години може видјети и посебна криминалистичка обрада кроз коју се врши идентификација кривичних дјела и извршилаца који злоупотребљавају материјал сексуалног злостављања и искориштавања дјеце сачињен употребом алата базираних на вјештачкој интелигенцији;
* различите врсте превара гдје истичемо преваре које се односе на злоупотребу пословне имејл коресподенције, преваре са картицама за безготовинско плаћање, преваре са информацијама о намјештеним спортским мечевима, љубавне преваре, инвестицијске преваре и слично.
* кривична дјела из области заштите ауторских права;
* кривична дјела из области неовлаштене трговине интелектуалним власништвом;
* кривична дјела извршења куповином роба и ислуга на „тамном вебу“, гдје се прије свега мисли на неовлаштену куповину и злоупотребу личних података, података о картицама за безготовинско плаћање, опојних дрога, фалсификованих новчаница и слично.

Такође, важно је напоменути да Министарство унутрашњих послова Републике Српске кроз готово све криминалистичке обраде остварује значајну међународну сарадњу како са појединим земљама тако и са међународним организацијама као што су INTERPOL и EUROPOL.

Надаље, Министарство унутрашњих послова Републике Српске је у протеклом периоду значајно ставило акценат на превентивним активностима, те истичемо сљедеће активности:

* Спровођење превентивно-едукативног програма „Дјеца у дигиталном добу и дигитално насиље“;
* Спровођење кампање „Стоп вршњачком насиљу“ са акцентом на спречавање насиља у дигиталном окружењу;
* Учествовање у радионицама на тему: „Роднозаснована кривична дјела у дигиталном окружењу“;
* Учествовање у различитим телевизијским емисијама информативног и едукативног садржаја на различите теме као што су заштита од превара, заштита дјеце од сексуалног злостављања и искориштавања и слично;
* Израда превентивно – едукативног материјала (фотографски, видео, штампани);
* Одржавање интернет презентације Јединице за високотехнолошки криминалитет.

Анализа података о сајбер криминалитету показује озбиљност и растући тренд овог типа преступа у друштву. Повећање броја регистрованих кривичних дјела и велика материјална штета која прати ова дјела указују на дубоке и сложене изазове с којима се суочавају правосудни системи и економије. Посебно је забрињавајуће што овакви криминални акти све више укључују нове технологије које омогућавају извршиоцима да дјелују без непосредног контакта са жртвама, чиме се значајно отежава њихова идентификација и процесуирање.

Од посебног значаја су кривична дјела која се односе на злоупотребу дигиталних платформи за искоришћавање дјеце у порнографске сврхе, као и други облици сексуалног злостављања путем рачунарских мрежа. Растући број таквих дјела представља озбиљну пријетњу за сигурност и физички интегритет дјеце, што захтијева хитну и снажну реакцију државних институција и друштва у цјелини. Поред тога, повећан број кривичних дјела који се односе на повреду приватности, као што су неовлашћено прислушкивање, фотографисање и злоупотреба личних података, наглашава потребу за већом заштитом основних људских права у дигиталном добу.

Један од најзначајнијих аспеката који проистиче из ове анализе је велика материјална штета која произилази из кривичних дјела као што су компјутерске преваре, прање новца и изнуда. Противправна имовинска корист која се остварује овим дјелима не само да наноси непосредну штету жртвама, већ има и шире економске посљедице. Компаније, али и појединци, доживљавају значајне финансијске губитке, што додатно компликује економску ситуацију и повјерење у електронске системе плаћања и трговине.

Растући тренд сајбер криминалитета поставља нове изазове у погледу законодавне регулације, али и у технолошкој и оперативној опремљености истражних и правосудних органа. За ефикасно сузбијање ових дјела, потребно је убрзано осавремењивање правног оквира и јачање институционалних капацитета. Такође, важно је повећати свијест грађана о опасностима које носи дигитално окружење, као и осигуравати већу заштиту за најрањивије групе, посебно дјецу, чија права су често угрожена овим облицима злочина.

Превенција је темељ успијешне борбе против сајбер криминалтета. Обуке и стручна усавршавања омогућавају полицијским службеницима и другим релевантним актерима да се упознају са најновијим техникама и алатима за сузбијање сајбер криминалитета, док семинари и округли столови подстичу размјену знања и искустава.

Пораст броја превентивних активности у 2023. години указује на улагање у јачање капацитета институција и сарадње са другим субјектима, што је кључно за ефективан одговор на све сложеније пријетње у дигиталном окружењу. Наставак овог тренда може допринjети не само већој ефикасности у сузбијању сајбер криминалитета, већ и бољем односу са заједницом кроз подизање свијести и едукацију.

Закључно, све ове чињенице указују на потребу за свеобухватним и координисаним приступом у борби против сајбер криминалитета, који ће омогућити већу заштиту грађана, посебно дјеце, као и осигурати очување основних људских права, као што су право на приватност и сигурност.

## **Стање и трендови сајбер криминалитета у Европи и свијету**

**Главне пријетње**

Растући волумен материјала о сексуалном злостављању дјеце на мрежи (*енг: CSAM*) представља све веће изазове за институције за спровођење закона које се боре против сексуалне експлоатације деце на интернету. Материјал са самостално генерисаним сексуалним садржајем чини значајан и растући дио материјала о сексуалном злостављању дјеце на мрежи који се детектује.

Затим, инвестицијске преваре, компромитовање пословних имејлова (*енг: BEC*) и љубавних превара и даље су најчешћи облици сајбер превара у ЕУ, с тим да је фишинг (*енг: phishing*) и даље најпревалентнији вектор напада. Дигитално скимовање представља сталну пријетњу која доводи до крађе, препродаје или злоупотребе података о кредитним картицама.

Алати и услуге засноване на вјештачкој интелигенцији (*енг: AI*) и машинском учењу постају уобичајени алати за сајберкриминалце и истичу се као производи на тржишту криминала као услуге (сајбер криминал као сервис, *енг: CCaaS*). Пријављени су случајеви материјала о сексуалном злостављању дјеце на мрежи који су потпомогнути, измијењени или генерисани уз помоћ вјештачке интелигенције, а у скорој будућности очекује се повећање броја евидентираних случајева. Алати засновани на вјештачкој интелигенцији и „дубоке лажи“ (*енг: deepfakes*) такође усавршавају способности превараната за социјални инжењеринг.

Као резултат глобалног рада институција за спровођење закона усмереног на криминалну инфраструктуру везану за рансомвер (*енг: ransomware*), рансомвер групе су се подијелиле и реорганизовале под различитим маскама.

**Извршиоци кривичних дјела**

Број извршилаца кривичних дјела наставља да расте, како због нових технологија које ефикасно смањују препреке, тако и због све веће сложености дигиталне инфраструктуре, која шири потенцијалну површину напада.

Криминални пејзаж и даље остаје широк, обухватајући и појединце и мреже са различитим нивоима стручности и способности. Неки сајберкриминалци који таргетирају ЕУ базирани су у ЕУ, док други дјелују са стране, скривајући своје незаконите активности и средства у трећим земљама.

Високоризични партнери и програмери остају важан ресурс, а различити провајдери рансомвера као услуге (*енг: RааS*) такмиче се за њихове услуге. Неки партнери се сумњиче да су развили сопствене варијанте рансомвера како би смањили своју зависност од рансомвер као сервис провајдера.

**Жртве кривичних дјела**

Милиони жртава широм ЕУ свакодневно су нападани и експлоатисани на мрежи. Рансомвер групе све више таргетирају мала и средња предузећа због слабије сајбер заштите. Интернет трговине и банке су префериране жртве напада дигиталног скимовања. Корисници и даље постају жртве фишинг кампања, компромитовања пословних имејлова, инвестиционих превара и љубавних превара. Број случајева онлине сексуалне изнуде који таргетирају рањиве малољетнике је, такође, у порасту.

Вишеслојни модели изнуде постају све чешћи у цјелокупном спектру сајберкриминалних пријетњи. Незаконита трговина личним подацима повезана је због честе појаве жртава који падају на поновљене преваре.

**Помагачи сајбер криминала**

„Тамни веб“ (*енг: dark web*) и даље представља кључни фактор за сајбер криминал, омогућавајући преступницима да дијеле знање, алате и услуге на скривенији начин. Као резултат тога, животни циклус криминалних сајтова је постао краћи, а сајтови-рефлектори се брзо појављују како би се супротставили уклањању. Тор (*енг: Tor*) мрежа остаје најпопуларнија платформа за сајбер криминалце за приступ „тамном вебу“.

Сајбер-криминална злоупотреба легитимних апликација за размјену порука са криптовањем (*енг: Е2ЕЕ*) наставља да расте. Криминално тржиште за рансомвере, малвере и фишинг као сервис расте и подсјећа на динамику легитимне индустрије, са сајбер криминалцима који објављују своје услуге путем „тамног веба“ и кроз криптовану комуникацију.

**Криптовалуте**

Употреба криптовалута у бројним областима криминала постала је очигледнија. Биткоин (*енг: Bitcoin*) је и даље криптовалута коју криминалци највише злоупотребљавају, али изгледа да употреба „алтернативних кованица“ (*енг: altcoin*) расте. Чини се да подземно банкарство за прање крипто имовине расте, заједно са поновним појављивањем дебитних картица за криптовалуте и редовном криминалном употребом услуга размјене.

Криминална употреба криптовалута постала је очигледнија 2023. године, као и број захтјева за истраживачку подршку које је Еуропол примио. Финансијска кривична дјела, углавном инвестиционе преваре и прање новца, остају подручје у којем се криптовалуте најчешће сусрећу. Фактори попут повећања вриједности одређених криптовалута и растуће медијске пажње према криптоинвестицијама такође доприносе сталном порасту броја случајева инвестицијских превара.

Главне врсте криптовалута са којима се сусрећемо, а посебно у инвестиционим преварама, као што је Биткоин се све више претвара у стабилне криптовалуте, вјероватно зато што су ове посљедње мање подложне цјеновној волатилности. Истражиоци су чешће наилазили на стабилну кованицу Тетер (*енг: Tether*) на Трон блокчејну (*енг: blockchain),* у односу на Етереум (*енг: Ethereum*), вјероватно због ниских трансакцијоних накнада на Трон мрежи. Неке стабилне криптовалуте су уградиле функционалност стављања на црну листу у своје паметне уговоре, што омогућава институцијама за спровођење закона да затраже од компанија да замрзну стабилне криптовалуте које су идентификоване као дио новчаника осумњиченог.

Оператери рансомвера углавном траже Биткоин као откупнину, јер га је још увијек лакше набавити него друге врсте криптовалута. Међутим, постоје случајеви у којима су захтјеви за откупнином упућени у другим крyптовалутама (нпр. Монеро). Криминална употреба алткоинова (алтернативне крyптовалуте) чини се да расте. Број случајева подржаних од стране Еуропола који укључују само Биткоин скоро је једнак броју случајева који су такође укључивали алтернативне криптовалуте.

Учешће несарадљивих пружалаца услуга остаје један од главних изазова у многим истраживањима која се односе на крyптовалуте. Док су неке компаније побољшале сарадњу са институцијама за спровођење закона, несарадљиви пружаоци услуга са сједиштем у офшор јурисдикцијама често доводе до дугих процедура међународне правне помоћи (*енг: MLA*). Новопримљена правила ЕУ о информацијама које прате трансфере средстава – дио пакета законодавних приједлога за јачање ЕУ закона против прања новца и финансирања тероризма – проширују обавезе извјештавања на пружаоце услуга криптовалута (*енг: VASP*). Правила ЕУ усвојена су у јануару 2024. године, а од тада је Европска банка за обнову такође проширила своје смjернице за ризик од прања новца и финансирања тероризма на пружаоце услуга повезаних са криптовалутама. Ови развојни догађаји вјероватно ће имати позитиван утицај на количину информација доступних органима реда у истрагама које се односе на криптовалуте, барем када су осумњичени лоцирани у ЕУ.

Прање новца помоћу крyптовалута, сложеност техника које се користе приликом прања криптовалута у великој мјери зависи од врсте кривичног дјела које је почињено. Случајеви инвестицијских превара који укључују криптовалуте често користе мање сложене методе, јер се већина тога обавља путем традиционалних облика (тј. путем тзв. „мула“, међународних банковних рачуна, кретања готовине и подземног банкарства), а не путем криптовалута.

Групе на апликацијама са криптованом комуникцијом су, све чешће, замјена за „peer-to-peer“ платформе за повезивање људи који желе да размене криптовалуте за готовину (и обрнуто, нпр. готовину за криптовалуте) и избјегну провјере усклађености. Рјешења подземног банкарства и криминални излази за прање имовине такође су у порасту. Поново су се појавиле и криптовалутне дебитне картице, јер се оне могу користити за брзо претварање криптовалута у готовину на банкоматима.

Године 2023. забиљежен је пораст употребе услуга за размјену у циљу прања криптовалута. Размјена се углавном врши како би се осигурао и стабилизовао криминални новац – за сигурност, криптовалуте се размењују за приватне криптовалуте (нпр. Монеро), док се за стабилност, криптовалуте размењују за стабилне криптовалуте (нпр. USDT). Да би се ускладиле са прописима, услуге за размјену често пружају институцијама за спровођење закона информације о поријеклу, конверзији и одредишној адреси.

**Тамни веb**

Тор мрежа и даље је најпопуларнији начин за сајберкриминалце да приступе тамном вебу, упркос напорима да се промовише „*Invisible Internet Project*“ као рјешење које је отпорније на надзор од стране институција за спровођење закона.

Форуми на тамном вебу и даље су главни канал за оглашавање тржишта на тамном вебу, иако нека тржишта такође имају сајтове и на површинском вебу. Администратори су наставили да ограничавају величину и животни вијек својих тржишта како би избјегли надзор институција за спровођење закона, док истовремено покушавају да одржавају велику базу корисника кроз изградњу добре репутације путем форума. Међу разлозима за кратак вијек тржишта на тамном вебу су често сусретани случајеви када администратори изненада затворе тржиште и украду сва средства која су држана код њих.

Форуми и „собе за комуникацију“ (*енг: chat rooms*) на тамном вебу и даље су кључни мрежни простори за извршиоце кривичних дјела у вези са сексуалном експлоатацијом дјеце да дискутују о материјалу сексуално експлоатисане дјеце и оперативној сигурности. Форуми на тамном вебу за извршиоце кривичних дјела у вези са сексуалном експлоатацијом дјеце постају све специјализованији према специфичним сексуалним преференцијама.

**Рансомвер као сервис**

LockBit је и даље био један од најпродуктивнијих рансомвер као сервис провајдера на тржишту 2023. године. Група је срушена у фебруару 2024. године захваљујући координисаним операцијама институција за спровођење закона из 10 различитих земаља, уз подршку Еуропол-а и Еуроџаст-а. Органи реда су омели рансомвер групу на сваком нивоу, озбиљно оштетивши њихове способности и кредибилитет. Претходна популарност *LockBit-а* могла се приписати њиховом сталном издавању нових функција на њиховој платформи и варијанти њиховог малвера. *LockBit* 3.0, познат као *LockBit Black*, који је укључивао нове функције (нпр. самоскривање), лансиран је 2022. године. У 2023. години, *LockBit* је издао *LockBit Green*, ажурирану варијанту рансомвера дизајнирану да циља виртуелне рачунарске и складишне услуге. Поред тога, рансомвер оператер је такође развијао енкриптор-е за циљање *MacOS* уређаја.

Једна рансомвер као сервис група која се појавила почетком 2023. године је Акира, коју истраживачи пријетњи повезују са сада расформираном Конти групом. С обзиром на брз раст базе жртава Акире и њихове зреле оперативне способности, вероватно ће постати све већа пријетња у блиској будућности.

**Малвер као сервис**

Током 2023. године дошло је до неколико промена у пејзажу малвер као сервис услуге (*енг: МааС*). Након гашења инфраструктуре *Qakbot* малвера, сајберкриминалци су брзо реаговали и окренули се другим добро успостављеним или новим провајдерима услуга. Значајне алтернативе *QakBot-у* које тренутно користе сајберкриминалци су *IcedID, SystemBC, Pikabot* (нови, који се појавио 2023. године), *DanaBot* и *Smokeloader* (који је интензивно коришћен од стране „*8base“* групе у њиховим кампањама), а ове услуге нуде сличне могућности за доставу злонамерних малвера на заражене системе.

Легитимни оквири за пенетрацијско тестирање, као што су *Cobalt Strike, Metasploit* и *Mimikatz*, широко се злоупотребљавају од стране сајберкриминалаца за успостављање постојаности и ескалацију привилегија унутар компромитованих система. *Cobalt Strike* је већ неко вријеме био најчешће коришћено рјешење због свог разноврсног арсенала способности. Користи се као бекдор и контролно-командни центар за извршавање команди, испоруку додатних и прелазак кроз инфилтриране мреже. Новији алати базирани на вјештачкој интелигенцији *PentestGPT* и слични, такође се могу користити са злонамјерном намјером за олакшавање иницијалне компромитације информационих система.

**Експлоатација дјеце на интернету**

Кључне пријетње које произилазе из онлајн експлоатације дјеце остале су релативно стабилне током 2023. године. Спољни фактори, као што су усвајање нових технологија и све већа присутност дјеце на мрежи без надзора, као и промјене у фокусу истраживачког рада, допринјели су еволуцији пријетњи које ово кривично дјело носи.

Материјал сексуално експлоатисане дјеце наставља да се шири на интернету, непрестано виктимизујући дјецу коју приказује. Са растућим обимом материјала које је потребно ручно анализирати и повезаних информација о случајевима, институције за спровођење закона се суочавају са потребом за иновативном технолошком подршком како би истраживали материјал сексуално експлоатисане дјеце. Производња и ширење материјала сексуално експлоатисане дјеце остаје озбиљан проблем, са великим дијелом материјала који је сада идентификован као самостално генерисан експлицитан материјал.

Уживо, даљинско злостављање дјецепредставља константну пријетњу, гдје починиоци гледају сексуално злостављање дјеце на захтјев, уз подршку једног или више саизвршилаца који врше злостављање над жртвом за новац. Овај облик злостављања је главна форма комерцијалне сексуалне експлоатације дјеце и главни извор непознатог материјала сексуално експлоатисане дјеце, што подразумијева тајно снимање жртве (нпр. у видео позиву).

Транснационални починиоци сексуалног злостављања дјеценастављају да врше злостављање дјеце док путују у и/или бораве у такозваним високоризичним земљама за жртве, гдје се повезују са својим циљевима. Они дјелују међународно, понекад у сарадњи са мрежом колега и уз подршку локалних саизвршилаца на различитим локацијама. Такви починиоци су добро повезани и производе значајну количину оригиналног материјала сексуално експлоатисане дјеце који се даље шири унутар заједнице починилаца на интернету, у којој често играју значајну улогу.

**Форуми и „собе** за комуникацију“ остају кључни мрежни простори за **починиоце сексуалне експлоатације дјеце**, који размјењују материјал сексуалне експлоатације дјеце и дискутују о злостављањима и фантазијама, како да прибаве оригинални материјал сексуално експлоатисане дјеце, техникама за манипулацију дјеце и савјетима о оперативној сигурности. Искуснији починиоци обично се повезују у форумима на „тамном вебу“ који постају све специјализованији и прилагођени сексуалним преференцама. Ови починиоци имају све виши ниво техничког знања и користе мјере за прикривање својих трагова. Форуми често имају специјализоване секције за техничка питања и заштиту, са савјетима и опцијама за обуку. Пошто су ови дигитални простори често подложни акцијама од стране институција за спровођење закона и различитим нападима, обично им животни вијек не прелази двије године. Да би превазишли ове препреке, администратори ових форума креирају двоструке **сајтове**, који чувају копију садржаја, а када им сајт буде уклоњен, брзо га поново постављају на нову адресу.

**К**риптоване платформе за комуникацију све више користе починиоци за размену материјала сексуално експлоатисане дјеце и комуникацију.

Обим **самостално генерисаног сексуалног материјала** сада чини значајан и растући дио материјала сексуално експлоатисане дјеце који се открива на мрежи. Овај садржај праве и приказују дјеца, посебно тинејџери. У многим случајевима, то је резултат добровољних размјена међу вршњацима, али се може класификовати као материјал сексуално експлоатисане дјеце када се дистрибуира трећим странама без пристанка особе која га је првобитно послала. **Самостално генерисани сексуални материјал** такође је често резултат онлајн сексуалне манипулације и уцјене. У овом контексту, починиоци идентификују жртву онлајн, често на платформама за игре или друштвеним мрежама, а након што стекну њихово повјерење кроз манипулацију, починиоци добијају сексуално експлицитан материјал и користе га као средство за уцјену. Осјећај срама и нада да ће пријетње престати често наводе жртве да праве још више самостално генерисаног сексуалног материјала.

Поред уцјењивања за нови материјал сексуално експлоатисане дјеце, неки починиоци такође захтијевају новац од својих жртава. Кроз сличан криминални процес, починиоци се упуштају у разговоре са жртвама претварајући се да су вршњаци који траже романтичну везу, а затим се претворе у **уцјењиваче.** Када жртве постану емоционално уплетене након што извршиоци добију први експлицитни снимак од малољетника, почињу да прете жртви, пријетећи да ће дијелити експлицитни снимак на мрежи или га послати блиским контактима жртве. Жртва, често осјећајући стид, може пристати да плати прекршиоцу како би спријечила да се то деси. Овај процес уцјене може трајати дуго, јер прекршиоци често захтјевају још експлицитних снимака или новац од жртве.

Онлајн групе које дијеле насилни и сексуални садржај, често смјештене на криптованим комуникационим платформама, такође су идентификоване као главна мјеста за **сексуалну уцјену**. Ове групе често функционишу као секте, где харизматични лидери манипулишу и обмањују чланове, чинећи их зависним и послушним. Чланови су подстакнути да дијеле екстремне видео записе или слике из страха, манипулације или због прихватања неприкладног понашања од стране групе. Извршиоци често уцјене жртве за додатни материјал, вршећи притисак на њих да производе још експлицитнијих и/или екстремнијих садржаја везаних за самоповређивање, што понекад раде уживо за забаву других чланова групе.

Неки извршиоци у овим групама су идентификовани као малољетници, који подстичу и наводе на производњу и дистрибуцију насилног садржаја, укључујући материјал сексуално експлоатисане дјеце.

Коришћење вјештачке интелигенције за генерисање или измјену фотографија брзо је еволуирало, а такви модели се све више злоупотребљавају од стране извршилаца за производњу материјала сексуално експлоатисане дјеце и за **сексуалну уцјену**. Ови алати сада могу креирати материјал који је врло сличан стварном материјалу сексуално експлоатисане дјеце, што га чини теже препознатљивим од стварног садржаја. У 2023. години, материјал сексуално експлоатисане дјеце креиран уз помоћ вјештачке интелигенције је већ пријављен и очекује се да постане значајан проблем у будућности.

Овај тип садржаја представља озбиљан изазов за инситуције за спровођење закона у идентификовању стварних жртава и одређивању правног оквира под којим би истрага требало да се води. Чак и када је материјал потпуно вјештачки и нема стварне деце, производња и дистрибуција материјала сексуално експлоатисане дјеце потпомогнут вјештачком интелигенцијом и даље доприноси ширем проблему сексуализације и објективизације деце.

Лака доступност и брзина којом се може производити материјал сексуално експлоатисане дјеце помоћу вјештачке интелигенције у комбинацији са ниским техничким захтјевима за стварање таквог садржаја, чине ово озбиљном пријетњом. То омогућава ширем спектру прекршилаца да стварају и шире незаконит материјал. Фотографије и видео материјал генерисани путем вјештачке интелигенције лако се може дистрибуисати на мрежи, повећавајући обим материјала сексуално експлоатисане дјеце у циркулацији и компликујући напоре у идентификацији жртава и извршилаца.

Како употреба алата базираних на вјештачкој интелигенцији за ове сврхе расте, тако ће бити потребна побољшана **форензичка** техника и правне стратегије за рјешавање овог еволуирајућег и узнемирујућег тренда онлајн експлоатације.

**Онлајн преваре**

Онлaјн преваре представљају растућу претњу у ЕУ и шире, што доводи до тога да милиони грађана ЕУ буду циљани, а милијарде евра украдене. Преваре у инвестицијама и компромитација пословних имаилова остају најпрофитабилније онлајн преваре. Доступност услуга попут фишинга расте, док дигитално скимовање представља још једну значајну пријетњу, посебно за трговце на интернету.

**Фишинг**

Фишинг је остао најчешће коришћен вектор напада међу онлајн преварама у 2023. години. Смишинг (фишинг путем СМС порука) био је најчешћи облик фишинга, испред других варијанти попут вишинга (фишинга путем позива) и спуфинга. Q-ишинг, или QR код фишинг, такође се појавио 2023. године. Q-ишинг, или QR код фишинг је фишинг напад који користи лажне QR кодове умјесто линкова заснованих на тексту, као у традиционалним фишинг преварама. Преваранти такође постављају лажне QR кодове на физичким локацијама које жртве скенирају.

Фишинг као сервис представља индустрију која брзо расте. Овај тржишни модел нуди производе, услуге и податке жртава, што омогућава све већем броју криминалних мрежа да се успјешно баве овом криминалном активношћу, без обзира на њихов ниво организације и техничке стручности. Свако може затражити фишинг страницу за било коју банку или пошту у ЕУ. Криптовалуте су најчешћи метод плаћања за основне или премиум претплате на овакве услуге.

Осим најпревалентнијих облика фишинга, позната преварантска шема која је порасла у 2023. години укључивала је хиљаде дневних „шок позива“ са социјалним инжењерингом и позивним центрима. Овај масовни феномен циљао је стотине хиљада људи широм ЕУ. Криминалне мреже које дјелују и унутар и изван ЕУ, преко различитих локалних сарадника, стоје иза ове шеме.

**Преузимања рачуна**

Недавна истраживања показују растућу пријетњу од илегалне трговине личним подацима као кључног облика концепта „криминал као сервис“ (*енг: CaaS*). Преузимање налога и даље је циљ за нападе на рачуне жртава (онлајн банкарство, имаил налоге или профиле на друштвеним мрежама). Кроз преузимање налога, криминалци такође могу преузети средства и приступити дигиталним услугама жртава или осјетљивим приватним информацијама које се затим могу уновчити онлајн. Како банке све више третирају губитке новца кроз превару са двоструком аутентификацијом и креденцијалима као немар легитимног власника налога, преварантске шеме које циљају на рачуне појединаца остају ниско-ризичне и високо-профитабилне активности за криминалце.

**Инвестиционе преваре, пословна имејл коресподенција и љубавне преваре**

Инвестициони преваранти и даље представљају кључну претњу у ЕУ, циљајући на хиљаде жртава и генеришући милионске илегалне профите. Криптовалуте настављају да буду најчешће пријављени производ који се нуди жртвама у инвестицијским преварама.

Алати за даљинску администрацију су кључни за преваранте који воде ове шеме путем уређаја жртава. Постоје криминалне инвестиционе апликације које су доступне за преузимање на легитимним продавницама апликација у различитим земљама и језицима. Огласи генерисани помоћу вјештачке интелигенције такође се користе као мамац за потенцијалне жртаве и овај вид криминалитета ће вјероватно расти.

Компромитација пословне имејл коресподенције (*енг: Business Email Compromise – BEC*), а посебно превара са извршним директорима (*енг: CEO fraud*), и даље је често пријављивана врста преваре против грађана ЕУ и приватних компанија. У неким случајевима, преваранти користе фишинг технике за пресретање и манипулацију корпоративним комуникацијама. Увјерљиви преварантски имејлови могу се лако генерисати уз помоћ великих језичких модела. С обзиром на растућу популарност генеративних модела базираних на вјештачкој интелигенцији, у 2023. години откривени су неетични велики језички модели који ће се вјероватно развијати.

Иако је ниво пријављивања низак, углавном због осјећаја срама који осећају жртве, превара путем романтичних превара и даље представља велику пријетњу. Алати базирани на вјештачкој интелигенцији проширују могућности за преваранте не само да дођу до више жртава истовремено, већ и да унаприједе своје технике социјалног инжењеринга.

**Напади дигиталног прескимеровања**

Дигитално прескимеровање остало је значајна пријетња у 2023. години, посебно у циљању веб сајтова интернет трговине. Починиоци убацују злонамерни код, познат као веб скимери, у веб сајтове онлајн продавница путем различитих метода и техника.

Напад дигиталног прескимеровања обично се састоји од три главне компоненте:

1. *Loader* – Почетни корак у којем се злонамерни код уводи на веб сајт.
2. Злонамерни нападни код – Штетан код, или веб скимер, који прикупља осетљиве податке.
3. Ексфилтрација података – Метод који се користи за слање украдених података на командно-контролни сервер нападача (*енг: C2 server*).

Веб скимери могу бити убачени директно на сервер циљаног сајта или искоришћавањем рањивости у платформи интернет трговине. Такође могу бити убачени на сајт путем напада на ланац снабдијевања, гдје нападач користи трећу страну као ресурс. У тим случајевима, ако страница садржи код са другог домена, нападач може убацити злонамерни код и заобићи већину сигурносних мјера. Процес ексфилтрације података осигурава да украдени подаци буду послати на командно-контролни сервер нападача, често без изазивања аларма.

**Преваре на банкоматима**

Преваре на банкоматима у ЕУ смањене су за 40% у првој половини 2023. године у поређењу са 2022. годином. Ово смањење је углавном резултат опадања напада с циљем блокирања готовине које су извршавали преваранти на банкоматима (постављањем поклопца испред утора тако да новац не може да изађе из машине). Напади на информациони систем настављају да се догађају, што доводи до напада на банкоматима са циљем повлачења готовине.

**Онлајн преваре и прање новца**

Преваре, нарочито оне везане за инвестиције, и даље представљају најчешће идентификоване основне прекршаје повезане са илегалном употребом криптовалута. Како преваранти усавршавају технике прикривања за прање новца, све више се ослањају на дигитална банкарска рјешења, подземно банкарство и криминалне финансије, као и на неусклађене пружаоце услуга криптовалута са недовољним нивоом процедура за верификацију идентитета (*енг: KYC*). Такође, злоупотреба виртуелних ИБАН бројева и даље представља потенцијалну растућу пријетњу. Међутим, новчани курири и друге традиционалне методе прања новца такође су се појавили у недавним истраживањима, са неким корацима криминалног процеса који се протежу кроз јурисдикције са недостацима у међународним стандардима против прања новца и сарадње са институцијам за спровођење закона.

**Очекивања**

Шира употреба алата базираних на вјештачкој интелигенцији и услуга од стране сајберкриминалаца ствара нове пријетње, укључујући злоупотребу легитимних алата и услуга, као и њихове злонамерне верзије које криминалци праве ad-hoc. Растући број великих језичних модела без филтрирања упита који су се недавно појавили, вјероватно ће се мултиплицирати, а све је већа вјероватноћа да ће бити више огласа направљених уз помоћ алата базираних на вјештачкој интелигенцији који привлаче потенцијалне жртве у онлајн преваре. Коришћење вјештачке интелигенције за побољшање криминалних метода и скрипти (на пример, за хаковање дигиталних берзи и ликвидносних протокола у циљу крађе средстава) представља још један могући сценарио. Злоупотреба великих језичких модела могла би омогућити криминалцима да превазиђу језичке баријере, па би извршиоци кривичних дјела могли да врше онлајн манипулацију жртвама на било ком језику, претварајући се да су вршњаци и комуницирајући на начин који жртве перципирају као природан и уверљив. Злонамјерни велики језички модели постаће још истакнутији унутар оквира „криминала као услуге“.

Материјал сексуално експлоатисане дјеце креиран уз помоћ алата базираних на вјештачкој интелигенцији представља још једну забрињавајућу пријетњу која ће захтјевати пажљиво праћење. Примењени алати базирани на вјештачкој интелигенцији за модификацију и креацију потпуно вештачког материјала сексуално експлоатисане дјеце представљаће растуће изазове за истраге органа за спровођење закона, не само у погледу обима материјала сексуално експлоатисане дјеце који је у оптицају, већ и способности истражилаца да идентификују стварне идентитете жртава и починилаца. Алати базирани на вјештачкој интелигенцији ће смањити препреке за улазак у сајберкриминал, што значи да ће појединци са ограниченим техничким знањем моћи да изврше сајбер нападе и оркестрирају прилично софистициране онлајн преварантске шеме.

Сајберкриминалци који се баве сексуалном експлоатацијом деце и онлајн преварама и даље ће искоришћавати „deepfake“ технологију, јер њен квалитет расте и постаје лакша за употребу. Таква технологија би могла бити злоупотребљена у случајевима сексуалне изнуде, јер починиоци стварају лажни садржај како би пријетили жртвама. Овај тренд ће захтијевати да органи за спровођење закона имају прикладније и софистицираније алате за идентификацију који (дијелови) аудио, фотографског и видео садржаја су заправо лажни.

Главне платформе за криптовану комуникацију све више користе извршиоци кривичних дјела. Тренутни регулаторни оквир у вези са заштитом личних комуникација путем криптовања ствара изазове за законит приступ органа за спровођење закона до криминалних комуникација.

Шира примена Web3 принципа доводиће до даље децентрализације Интернета. У децентрализованом интернету, комуникације нису под контролом ни влада ни приватних компанија. Технологија *blockchaina* и *P2P* мреже су два типа децентрализованих комуникационих мрежа које се састоје од платформи које су у приватном власништву и којима управљају корисници. Децентрализација, *blockchain* технологија и *P2P* мреже и даље ће пружати могућности сајбер преступницима јер олакшавају спровођење трансакција анонимно и ван видокруга власти.

Очекивати је да ће се појавити нови рансомвер као сервис брендови, али ће њихов опстанак у великој мјери зависити од искуства и софистицираности криминалних актера иза тих операција. Пошто многе групе за рансомвер дјелују у земљама са ограниченом судском сарадњом, приступ органа за спровођење закона да ометају и уклањају криминалне услуге, како би посијали несигурност у вези са њиховим брендовима, биће кључна стратегија у будућности.

Актуелне реформе регулаторних механизама за платне услуге требало би да имају позитиван утицај на онлајн и платне преваре. У јуну 2023. године, Европска комисија је представила серију приједлога, укључујући и Директиву о платним услугама 3 и Уредбу о платним услугама. Директива о платним услугама подстиче платне институције да добровољно дијеле информације у вези са преварама ради боље међуинституционалне сарадње. Поред побољшања дијељења информација, директива о платним услугама проширује права на рефундацију за потрошаче који постану жртве спуфинг превара, где се преваранти лажно представљају као запослени платних институција.

Тренутна верзија Стандарда за сигурност података платних картица повући ће се 31. марта 2024. године, а нова верзија ће ступити на снагу у јуну 2025. Нова правила ће бити усмерена на јачање капацитета за спречавање већих скиминг напада. На примјер, предузећа која прихватају плаћање кредитним картицама мораће да буду свјесна којим скриптама раде на њиховим онлајн платним страницама, како се те скрипте понашају и када се промјене. Поред тога, интернет трговци који користе уградни оквир платних форми од трећих страна мораће да имају могућност да процене заглавља као и да открију неовлашћене промјене скрипти на самој платној страници, и да подигну узбуне за сваку промену скрипти.

Кључни инструмент ЕУ за борбу против онлајн претњи је ЕУ Дигитал Сервис Акт, који је ступио на снагу 17. фебруара 2024. Овај ЕУ регулативни оквир има за циљ да обезбједи сигурније искуство за све унутар онлајн екосистема, подстичући дигиталне услуге које послују у ЕУ да побољшају транспарентност и одговорност. Дигитал Сервис Акт се фокусира на онлајн платформе, претраживаче, хостинг услуге и посредничке услуге које нуде мрежну инфраструктуру, и утврђује број начина за борбу против илегалног садржаја, добара и услуга. То укључује обавезу онлајн тржишта да побољшају своје „познај свог купца“ праксе, увођење система за верификоване пријавиоце за фалсификоване и несигурне производе, забране огласа који таргетирају малољетнике или који су засновани на етничкој припадности, политичким ставовима или сексуалној оријентацији.

Неколико дешавања на тржишту криптовалута вероватно ће имати значајан утицај на злоупотребу криптовалута од стране криминалаца у многим облицима сајберкриминала у блиској будућности. У јануару 2023. године покретање Bitcoin ordinals омогућава корисницима да креирају незамењиве токене на Bitcoin blockchainu. За сада је технички тешко креирати ordinals, и вероватно неће бити масовно усвојени, али остају потенцијално искористиви од стране сајбер криминалаца. Такође, могу се појавити и друге криминалне пријетње у вези са биткоин ЕТФ-овима. Први биткоин ЕТФ је одобрен у јануару 2024. године, што ће омогућити инвеститорима да спекулишу о цијени биткоина без директног власништва над биткоинима. Овај развој може довести до ширег прихватања биткоина. Међутим, преваранти би могли злоупотријебити пораст ЕТФ-ова везаних за криптовалуте, јер ће људи без опсежног искуства у криптовалутама бити све више изложени тим инвестицијама. Компаније које издају крипто ЕТФ-ове такође ће морати да држе велике резерве у криптовалутама, што их може учинити вредним метама за преваранте.

**Обнова фокуса на превенцију**

Приоритизовањем превенције органи за спровођење закона и креатори политика могу се бавити сајберкриминалом у његовом основном облику, што води ка одрживим и дугорочним рjешењима у заштити сајберпростора. Фокусирањем на коренске узроке који подстичу појединце да се баве сајберкриминалним активностима, као што су недостатак свjести, финансијски подстицаји или социо-економски фактори, власти могу ефикасно смањити стопе онлajн криминала.

Инвестирање у превенцију преступника не само да смањује непосредне ризике које сајбер пријетње доносе, већ помаже и у стварању културе сајбер безбједности, што доприноси сигурнијем дигиталном окружењу за појединце, предузећа и владе.

Када се разматрају профили сајберкриминалаца, већина криминалаца су млади, посебно с обзиром на дисруптивну природу овог криминалног подручја и његов потенцијал за штету. Док њихови прекршаји штете њиховим жртвама, они такође имају потенцијално далекосежан утицај на њихову будућност, јер многи од тих појединаца нису свјесни правних посљедица онога што сматрају само изазовом или игром. Сајберкриминалци обично не сносе посљедице док не крену даље путем криминала, често се први пут сусрећући са органима за спровођење закона кроз лишење слободе. Њихове напредне дигиталне вјештине могле би бити преусмјерене ка законитом путу који би доприносио друштву. У ЕУ, превенција сајбер преступника добија све веће признање као кључна стратегија, уз истраживачке мјере, за ефикасну борбу против сајберкриминала.

У том оквиру, од 2023. године, Еуропол подржава мрежу *InterCOP*. Ова мрежа састоји се од међународних институција за спровођење закона, које дијеле стручност и заједнички развијају, имплементирају и процјењују интервенције и кампање за превенцију. Мрежа сарађује са јавним и приватним секторима чије су вјештине, ресурси и досег потребни, заједно са напорима институција за спровођење закона, да би се створило сигурније дигитално окружење.[[5]](#footnote-5)

## **Институционални механизми борбе против сајбер криминалитет**

Република Српска је успоставила властити институционални механизам за борбу против сајбер криминалитета који чине сва Министарства у влади Републике Српске заједно са Агенцијама и правосудним институцијама, гдје свако из домена своје надлежности спроводи репресивне и превентивне мјере са циљем спречавања и превенције сајбер криминалитета.

Међутим, примарни институционални механизам чине Министарство унутрашњих послова Републике Српске, заједно са Агенцијом за информационо-комуникационе технологије у чијем саставу се налази CERT Републике Српске, као први орган ове врсте у Републици Српској и Босни и Херцеговини, који у свом раду тијесно сарађује са Министарством унутрашњих послова Републике Српске, тужилаштвима и судовима. (Графикон број 6)

Графикон број 6. Приказ институционалног механизма борбе против сајбер криминалитета.

Министарство унутрашњих послова Републике Српске у свом саставу има специјализовану Јединицу за високотехнолошки криминалитет, организационо смјештену у Управи криминалистичке полиције, чији је дјелокруг рада откривање, доказивање и превенција свих облика сајбер криминалитета. (Графикон број 7)

Графикон број 7. Мјесто Јединице за високотехнолошки криминалитет у организационој структури институционалног механизма борбе против сајбер криминалитета унутар Министарства унутрашњих послова

Свеобухватност борбе против високотехнолошког криминалитета у Министарству унутрашњих послова Републике Српске се остварује кроз заједничко дјеловање Управе криминалистичке полиције - Јединице за високотехнолошки криминалитет, Управе за полицијску подршку – Јединице за форензику (врши вјештачења дигиталних уређаја и доказа) и Управе за информационо – комуникационе технологије (врши успоставу, одржавање и заштиту инфомационо – комуникационог система Министарства). (Графикон број 8)

Графикон број 8. Приказ институционалног механизма борбе против сајбер криминалитета унутар Министарства унутрашњих послова

Јединица за високотехнолошки криминалитет је организована на начин да има једну централну јединицу у сједишту Министарства у Бања Луци те по полицијским управама у зависности од величине и категорије полицијске управе у Бања Луци има Одсјек за високотехнолошки криминалитет, у полицијским управама Приједор, Добој, Бијељина, Зворник, Источно Сарајево и Требиње има по два инспектора за високотехнолошки криминалитет, те у полицијским управама Градишка, Мркоњић Град и Фоча има по једног инспектора за високотехнолошки криминалитет. Чиме је Министарство унутрашњих послова Републике Српске оперативно покрило цијело подручје свог оперативног дјеловања са посебно обученим полицијским службеницима из области борбе против сајбер криминалитета.

Осим тога, важно је напоменути и унутрашњу огранизацију саме Јединице за високотехнолошки криминалитет у сједишту која се састоји од једног Одјељења за високотехнолошки криминалитет, у чијем саставу су систематизована радна мјеста инспектора за високотехнолошки криминалитет, те два радна мјеста инспектора за превенцију високотехнолошког криминалитета, чиме је Министарство унутрашњих послова Републике Српске нагласило важност превентивног дјеловања у области сајбер криминалитета. (Графикон број 9)

Графикон број 9. Приказ организационе структуре Јединице за високотехнолошки криминалитет Министарства унутрашњих послова

Изазови сајбер криминалитета су велики, а вријеме извршења кривичних дјела у највећем броју случајева истовремено са наступањем посљедица, због чега се не може очекивати да једна држава или појединачни државни органи сами ријеше проблем сајбер криминалитета.

Управо из овог разлога потребно је повезивање свих институција са ширим контекстом превентивних и репресивних мјера, размјена података и информација између министарстава, партнерских агенција и друштва уопште, а све у циљу ефикасне борбе против сајбер криминалитета.

# **SWOT АНАЛИЗА И СТРАТЕШКО ФОКУСИРАЊЕ**

## **SWOT анализа**

Синтеза кључних налаза ситуационе анализе по тематским областима представљена је у наставку текста у виду прегледа снага/предности и слабости/недостатака, утврђених на бази чињеничног стања и уочених трендова. Уз кључне снаге и слабости идентификоване су и главне прилике/могућности као и пријетње из перспективе борбе против сајбер криминалитета у Републици Српској. Потенцијалне прилике и пријетње су препознате на основу процјене стања, сагледавања трендова вањских фактора утицаја и будућих очекивања. Заједно, ова четири прегледа (снаге, слабости, прилике и пријетње) су интегрисана у јединствену SWOT анализу.

Са методолошког аспекта, израда јединствене SWOT анализе помаже да се у наредним корацима израде стратешког документа лакше одреде кључна, стратешка усмјерења и то на начин да се будуће интервенције заснивају на утврђеним снагама, препознатим компаративним предностима и повољним приликама у окружењу, уз истовремено избјегавање пријетњи и отклањање главних слабости и недостатака.

**Табела 5.** SWOT матрица

|  |  |
| --- | --- |
| **S - (Strengths) СНАГЕ** | **W - (Weaknesses) СЛАБОСТИ** |
| * Стање безбједности у области сајбер криминалитета на задовољавајућем нивоу * Успостављен законодавни оквир за борбу против сајбер криминалитета * Успостављен стратешки оквир за борбу против сајбер криминалитета * Успостављен институционални механизам за превенцију сајбер криминала унутар МУП * Успостављена пракса специјализације полицијских службеника за борбу против сајбер криминалитета * Успостављен институционални механизам за одговор на безбједносне инциденте и пријетње * Образовни систем препознаје потребу за образовањем дјеце у области заштите у дигиталном окружењу | * Недовољна техничка опремљеност институција за спровођење закона * Одлазак обучених особа за супротстављање сајбер криминалитету из државног у приватни сектор * Недовољна специјализација особља у правосудним институцијама за борбу против сајбер криминалитета * Непостојање организационих претпоставки за борбу против сајбер криминала у правосудним институцијама * Недовољна информисаност и оспособљеност особља у институцијама (и предузећима) за препознавање и супротстављање различитим облицима сајбер криминалитета * Низак ниво сајбер безбједносне културе становништва * Недовољно развијен образовни систем на високошколским установама за образовање кадра за борбу против сајбер криминалитета |
| **O – (Opportunities) ПРИЛИКЕ** | **T - (Threats) ПРИЈЕТЊЕ** |
| * Унапријеђење нормативног оквира кроз усклађивање законске регулативе са европским и свјетским стандардима, израду подзаконских аката и процедура на супротстављању сајбер криминалитету * Израда властитих студијских програма за образовање кадрова у области борбе против сајбер криминалитета * Развој капацитета на пољу превенције сајбер криминалитета (превентивни рад усмјерити и према жртвама али и према извршиоцима кривичних дјела) * Развој капацитета на пољу информисања и подизања нивоа сајбер безбједносне културе код становништва * Развој дигиталних компетенција код становништва * Развој програма за подстицање корисног и креативног кориштења ИК технологија код дјеце и подизања нивоа информацијске писмености * Употреба алата на бази вјештачке интелигенције у истражне и образовне сврхе | * Повећање броја кривичних дјела у области сајбер криминалитета * Концепт „сајбер криминал као сервис“ који проширује структуру и повећава број извршилаца кривичних дјела * Употреба алата на бази вјештачке интелигенције за извршење кривичних дјела у области сајбер криминалитета * Употреба алата на бази вјештачке интелигенције за креирање лажних вијести, лажног садржаја, лажног фотографског и видео материјала сексуалног насиља и злостављања дјеце * Употреба софистицираних рачунара и рачунарске опреме за извршење кривичних дјела * Употреба криптовалута за извршење кривичних дјела сајбер криминалитета, прање новца и слично * Употреба апликација за комуникацију са криптованим садржајем * Децентрализација мреже кроз блокчејн технологију и клијент клијент концепт * Међународни карактер овог вида криминалитета * Висока материјална штета и негативан економски утицај овог вида криминалитета |

## **Стратешки фокуси**

Дефинисање стратешких фокуса представља корак у изради стратешке платформе којим се настоје одредити кључна усмјерења борбе против сајбер криминалитета.

Сходно томе, на основу кључних налаза претходне анализе стања и SWOT анализе предложени су сљедећи стратешки фокуси борбе против сајбер криминалитета:

**Стратешки фокус 1:** **Унапређење капацитета за репресивно дјеловање у области борбе против сајбер криминалитета у Републици Српској.**

Овај фокус подразумијева јачање институција и обуку кадрова како би се ефикасније супротставили свеприсутним пријетњама у дигиталном простору. Такође, укључује сарадњу са међународним организацијама и размјену информација ради побољшања одговора на сајбер криминалитет.

**Стратешки фокус 2:** **Унапређење капацитета за превентивно дјеловање у области борбе против сајбер криминалитета у Републици Српској.**

Унапређење капацитета за превентивно дјеловање у области борбе против сајбер криминалитета у Републици Српској има за циљ јачање система који ће спријечити и минимизирати ризике од сајбер напада и других облика дигиталног криминалитета. Овај фокус укључује развој и имплементацију превентивних мјера, као што су обука стручњака, унапређење информационе инфраструктуре и јачање свијести јавности о безбједности на интернету.

## **Стратешка визија**

**Стратешка визија је стварање повољног безбједносног амбијента који пружа могућност развоја и економске стаблиности Републике Српске и њено позиционирање међу земље с повољном пословном климом за инвестирање, оснаживањем дигиталних компетанција и свијести становништва у примјени информационо комуникационих технологија.**

Ова визија није линеарна већ развијена као процес који се у контексту брзих технолошких промјена стално прилагођава. Оствариваће се корак по корак, кроз координисану сарадњу јавног и приватног сектора, али и уз значајну укљученост академских и образовних институција. Уз стално унапређивање инфраструктуре и јачање капацитета полицијских и правосудних органа, ова стратегија ће кроз стратегију едукације, оснаживање дигиталних компетенција становништва, осавремењивања правних регулатива и развоја нових алата омогућити бржи и ефикаснији одговор на све нове изазове сајбер криминалитета.

Стварање повољног безбједносног амбијента пружа могућност за развој Републике Српске, инвестирање и јачање економске стабилности.

Као резултат ових напора, Република Српска ће се позиционирати међу земље са позитивном пословном климом, ниским нивоом опасности од сајбер напада, високим нивоом правне сигурности, технолошки напредном и привлачном за иновестиције.

Оснаживање дигиталне компетенције становништва омогућава кориштење инфомационо – комуникационе технологије за унапређење свих сфера друштвеног дјеловања, развијање иновативности и проналазаштва, те смањење ризика од опасности и угрожавања.

## **Стратешки циљеви**

На основу дефинисаних стратешких фокуса и предложене визије развоја, утврђују се сљедећи стратешки циљеви:

1. Превенција сајбер криминалитета кроз подизање нивоа сајбер безбједносне културе;
2. Унапријеђење законодавног оквира за борбу против сајбер криминалитета;
3. Развој и унапређење постојећих капацитета републичких органа (људски и материјално технички) за борбу против сајбер криминалитета;
4. Развој и унапређење сарадње између свих органа који учествују у борби против сајбер криминалитета;
5. Развој и унапређење међународне сарадње у циљу ефикасне размјене информација и заједничких истрага.

Међусобни однос стратешке визије и стратешких циљева може се представити следећим графиконом:

Развој и унапређење међународне сарадње у циљу ефикасне размјене информација и заједничких истрага

Позиционирање Републике Српске међу земље са позитивном пословном климом

Стварање повољног безбједносног амбијента који ће пружити могућност за развој

Развој и унапређење сарадње између свих органа који учествују у борби против сајбер криминалитета

Превенција сајбер криминалитета кроз подизање нивоа сајбер безбједносне културе

Унапријеђење законодавног оквира

Развој и унапређење постојећих капацитета републичких органа (људски и материјално)

Оснаживање дигиталне компетенције становништва

Графикон број 10. Приказ међусобног односа стратешке визије и стратешких циљева

Први стратешки циљ заснива се на стратешком фокусу, одређеном након ситуационе и SWOT анализе. С обзиром на убрзани развој информационог друштва при чему, како је приказано, сваки сегмент друштвеног и привредног развоја свакодневно користи информационе технологије, неопходно је континуирано радити на подизању нивоа сајбер безбједносне културе а самим тим и превенције сајбер криминалитета. Овим се олакшава уклапање у глобални тренд дигитализације цијелог друштва.

Други стратешки циљ такође се заснива на стратешком фокусу и има за циљ унапријеђење нормативног оквира кроз усклађивање законске регулативе са европским и свјетским стандардима, израду подзаконских аката и процедура којим би се на адекватан начин одговорило сајбер пријетњама.

Трећи стратешки циљ произилази из констатованих слабости у SWAT анализи. Како је констатовано да постоји недовољна техничка опремљеност институција за спровођење закона али и недовољан број обученог особља у институцијама које се супротстављају сајбер криминалитету и на послијетку одлазак обучених особа из државног у приватни сектор. Унапређење људских и материјално техничких капацитета републичких органа омогућиће адекватан одговор на све појавне облике сајбер криминалитета али ће у многоме помоћи и код превентивних активности планираних у наредном периоду.

Четврти и пети стратешки циљ подразумјевају унапређење сарадње између приватног, јавног сектора и цивилног друштва али и унапређење међународне и регионалне сарадње (прије свега у циљу спречавања сексуалне експлоатације дјеце и малољетних лица али и у циљу откривања и процесуирања извршиоца осталих кривичних дјела из области сајбер криминалитета).

1. „Службени гласник Републике Српске“, број: 63/21. [↑](#footnote-ref-1)
2. „Службени глансик Републике Српске”, број 94/21. [↑](#footnote-ref-2)
3. Циљеви SDG 3; SDG 9; SDG16; SDG 17 [↑](#footnote-ref-3)
4. Усвојена од стране Опште скупштине Уједињених народа 24. децембра 2024. године [↑](#footnote-ref-4)
5. Internet Organised Crime Threat Assessment (IOCTA) 2024 [↑](#footnote-ref-5)