Dezvoltarea cooperării internaționale în domeniul securității informaționale

Autor: Tatiana Busuncian

Dr., conferențiar universitar

Chișinău 2026

Conținuturi

Dezvoltarea cooperării internaționale

Analiza modalităților de colaborare între instituțiile naționale și internaționale pentru consolidarea securității informaționale și combaterea amenințărilor cibernetice transfrontaliere.

Direcții de colaborare

Identificarea și evaluarea principalelor domenii de cooperare internațională în prevenirea și combaterea criminalității informatice și terorismului cibernetic.

Asigurarea securității

Implementarea strategiilor de securitate informațională în Republica Moldova prin prisma standardelor și practicilor internaționale recunoscute.

Termeni-cheie: Cooperare internațională, acorduri de colaborare, securitate cibernetică, interese naționale, criminalitate informatică, terorism cibernetic

Obiective de referință

- să identifice căile de colaborare internaţională a instituțiilor responsabile de securitatea informațională în domeniul prevenirii și combaterii terorismului și criminalității transfrontaliere;
- să analizeze principalele direcții de colaborare în acest domeniu;
- să inițieze negocierilor privind semnarea acordurilor de cooperare la nivel internațional pentru îmbunătățirea capacității de răspuns în cazul unor atacuri cibernetice majore;
- să determine interesele naționale de securitate informațională în formatele de cooperare internaţională la care Republica Moldova este parte;
- să evalueze activitatea la programe internaţionale care vizează domeniul securităţii informaționale.

Perspective globale privind securitatea cibernetică 2026

Securitatea cibernetică este o frontieră în care colaborarea nu numai că rămâne posibilă, ci și puternică. Raportul din acest an examinează intersecția dintre adoptarea inteligenței artificiale și pregătirea cibernetică, precum și disparitățile emergente pe care le creează inovația. Pe frontul geopolitic, fragmentarea și preocupările legate de suveranitate remodelează cooperarea și încrederea între națiuni. Amenințările hibride și escaladarea atacurilor cibernetice reflectă volatilitatea crescândă a mediului global. Dintr-o perspectivă economică, accesul inegal la resurse și expertiză continuă să amplifice inegalitatea cibernetică.

Confruntându-se cu inovația rapidă în domeniul tehnologiei, combinată cu impactul transformator al inteligenței artificiale, forțele de aplicare a legii nu pot combate criminalitatea cibernetică în mod izolat. Protejarea comunităților acum depinde de o adevărată cooperare între mai multe părți interesate. Numai împreună putem fi cu un pas înaintea infractorilor și putem susține siguranța, drepturile și reziliența pentru un viitor digital sigur.

Global Cybersecurity Outlook 2026. Insight Report, Januari 2026

Evoluția criminalității informatice

Începuturile: anii '70 - perioada de apariție a criminalității informatice

Criminalitatea informatică reprezintă totalitatea infracțiunilor care pot fi comise prin intermediul sistemelor informatice și de rețea, constituind o provocare majoră pentru securitatea globală.

Această categorie de infracțiuni include:

- Atacuri asupra sistemelor informatice sau de rețea;
- Utilizarea abuzivă a sistemelor ca parte a unei infracțiuni;
- Atacuri dirigate împotriva infrastructurii informatice.

Evoluția tehnologiei a generat noi forme de criminalitate, necesitând adaptarea constantă a măsurilor de securitate și a cadrului legal internațional.

ŢINTE

- organizaţiile internaţionale
- autoritățile înalte ale puterii executive și legislative
- instituțiile blocului economic
- universitățile anumitor state
- organizaţii sociale
- sistemul bancar
- Obiecte ale infrastructurii critice

CATEGORIILE SURSELOR CRIMINALITĂȚII INFORMAȚIONALE

Hackerii. Persoanele cu un nivel ridicat de cunoștințe în domeniul tehnologiilor informaţionale și care petrec mult timp la calculator în căutarea vulnerabilităților sistemelor informatice

Hacktiviştii. Termenul «hacktivism» provine dintr-un compus din două cuvinte «hack» și «activism» și este folosit pentru a se referi la noul fenomen de protest social, care este un fel de sinteză a activității sociale, are ca scop să protesteze împotriva la orice

Criminali cibernetici. Persoanele care exploatează rețele de calculatoare pentru profit ilegal

Persoanele implicate în spionaj industrial

Teroriştii

Terorismul cibernetic: conceptualizare și evoluție

Definiția FBI (1997) - Agentul Mark Pollitt

> "Atacul premeditat, motivat politic împotriva informației, sistemelor informatice, programelor informatice și datelor, rezultând în violența împotriva țintelor noncombatante, de către grupări sub-naționale sau agenți clandestini"

Conceptualizarea modernă

Terorismul cibernetic - influențarea ilicită împotriva sistemelor informaționale, în scopul de a amenința viața, sănătatea sau proprietățile persoanelor nespecificate prin crearea condițiilor pentru accidente și dezastre tehnogene sau amenințarea reală a unui astfel de pericol.

Această formă de terorism prezintă caracteristici specifice: anonimatul atacatorilor, impactul disproporționat asupra infrastructurii critice și capacitatea de a provoca panică în masă prin perturbarea serviciilor esențiale.

În contextul transformărilor tehnologice accelerate, conceptualizarea și evoluția terorismului cibernetic evidențiază necesitatea unor răspunsuri coordonate la nivel global. Astfel, dezvoltarea cooperării internaționale în domeniul securității informaționale devine un element esențial pentru prevenirea, combaterea și gestionarea eficientă a amenințărilor cibernetice contemporane.

Contextul global al cooperării internaționale

Societatea actuală se caracterizează prin accelerarea proceselor de digitalizare și interdependența crescândă în domeniul informațional. Asistăm astăzi la o lume globală, complexă, dinamică, fapt determinat de mutațiile ce au loc pe fondul procesului de globalizare și al dependenței informaționale.

Globalizarea digitală

Dependența crescândă de tehnologiile informaționale creează noi forme de vulnerabilitate, necesitând mecanisme robuste de protecție și răspuns rapid la incidente.

Amenințări asymetrice

Entitățile rău-voitoare exploatează vulnerabilitățile sistemelor pentru comiterea de infracțiuni, spionaj și atacuri asupra infrastructurii critice.

Reziliența națională

Fiecare stat trebuie să dezvolte capacități proprii de răspuns, integrându-le în mecanismele de cooperare internațională pentru eficacitate maximă.

Imperativul cooperării internaționale

Fundamentul juridico-instituțional

În domeniul securității informaționale se înscriu demersurile de creare a unui cadru legislativ și instituțional corespunzător cerințelor contemporane, cu impact strategic asupra evoluțiilor pe termen mediu și lung în plan național și internațional.

Dezvoltarea acestui cadru presupune armonizarea legislației naționale cu standardele internaționale, crearea de instituții specializate și implementarea de mecanisme eficace de monitorizare și răspuns la amenințări.

Evaluarea amenințărilor informaționale globale

Existența la nivelul fiecărui stat a unui cadru normativ robust în domeniul securității informaționale devine esențială în contextul escaladării amenințărilor la nivel global.

Componentele evaluării riscurilor

- **Riscurile statale și criminale** - interesul entităților în compromiterea infrastructurilor critice informaționale
- **Vulnerabilitățile sistemelor** - deficiențe software și factorul uman în securitatea cibernetică
- **Cultura de securitate** - nivelul de pregătire și conștientizare a utilizatorilor

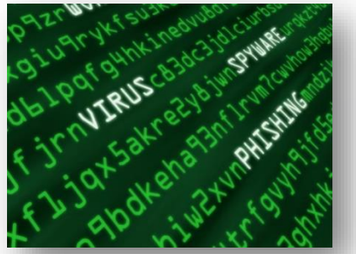
Această evaluare complexă permite identificarea zonelor de risc maxim și prioritizarea măsurilor de protecție și a investițiilor în securitatea informațională.

Provocări în implementarea legislației de securitate

Balanța între securitate și libertățile civile

Opiniile privind necesitatea unei legislații în domeniul securității informaționale variază considerabil, reflectând tensiunea inerentă între imperativele de securitate și protecția drepturilor fundamentale.

Preocupări legitime:



- Încălcarea dreptului la intimitate personală
- Limitarea libertății de exprimare în mediul online
- Restricționarea secretului corespondenței digitale
- Constrângerile impuse de autoritățile competente

Rezolvarea acestor dileme necesită o abordare echilibrată care să garanteze securitatea fără a compromite valorile democratice fundamentale ale societății deschise.

Educația și cultura de securitate informațională

Calculatorul oricărei persoane fizice care nu posedă cunoștințe minime în domeniul securității informaționale poate deveni ținta unui atac sau poate fi utilizat pentru atacuri cibernetice, fără ca proprietarul să conștientizeze acest lucru.

Educarea societății civile

Creșterea culturii de securitate prin programe educaționale comprehensive care să acopere toate segmentele societății.

Consolidarea încrederii

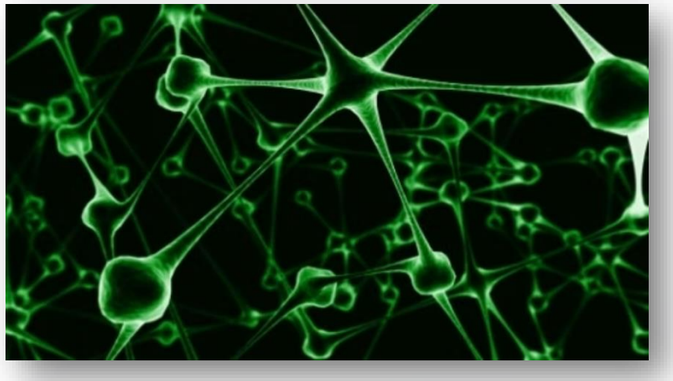
Dezvoltarea unui climat de încredere între instituțiile statului și societatea civilă pentru cooperarea eficientă în domeniul securității.

Modernizarea curriculei

Actualizarea programelor educaționale la nivel gimnazial și pregătirea personalului din administrația publică în domeniul securității informaționale.

Formarea magistraților

Dezvoltarea competențelor specializate în rândul judecătorilor și procurorilor pentru tratarea eficientă a criminalității cibernetice.



Clasificarea criminalității informatice

Clasificarea ONU

- Crime împotriva sistemelor informatice
- Crime comise pe sau prin intermediul calculatoarelor

Abordări regionale

Sisteme de clasificare dezvoltate la nivel regional pentru adaptarea la specificitatea juridică locală

Convenția Consiliului Europei privind criminalitatea informatică
Clasifică criminalitatea informatică în felul următor:

- Crime impotriva sistemelor informatice
- Crime comise pe sau prin intermediul calculatoarelor
- Infracţiuni referitoare la conţinut
- Infracţiuni referitoare la atingerile aduse proprietătii intelectuale şi drepturilor conexe

diseminarea informației rasiste și alt caracter, care incită la violență, ură sau discriminare împotriva unei persoane sau a unui grup de persoane pe criterii de rasă, naționalitate, religie sau etnie.

- Convenția CE din 23/11/2001 privind criminalitatea informatică

http://infoeuropa.md/criminalitatea-informatica/

Securitatea informatică - Abordare sistemică

Fiecare stat utilizează un set comprehensiv de instrumente, politici, principii, măsuri de siguranță, abordări de gestionare a riscurilor, acțiuni, programe de formare, experiență acumulată, sisteme de asigurare și tehnologii avansate pentru protejarea spațiului informatic și a resurselor organizaționale și ale utilizatorilor.

Componente esențiale:

- **Politici de securitate** - cadre normative clare și aplicabile
- **Tehnologii de protecție** - soluții hardware și software avansate
- **Formarea personalului** - dezvoltarea competențelor specializate
- **Gestionarea riscurilor** - metodologii de evaluare și mitigare
- **Monitorizarea continuă** - sisteme de detectare și alertă timpurie

Convenția privind criminalitatea informatică - Obiective strategice

1 Armonizarea legislativă

Adoptarea unei legislații adecvate și îmbunătățirea cooperării internaționale referitor la infracțiuni și dispoziții relevante în domeniul criminalității informatice și prevederilor în domeniul criminalității cibernetice

2 Competențe judiciare

Stabilirea competențelor și procedurilor necesare pentru investigarea și urmărirea penală pentru aceste infracțiuni, precum și pentru alte infracțiuni săvârșite prin intermediul sistemelor informatice

3 Colectarea probelor digitale

Dezvoltarea metodologiilor și instrumentelor pentru colectarea, analizarea și prezentarea probelor în format electronic în procesele judiciare

4 Cooperarea internațională

Elaborarea mecanismelor de cooperare internațională rapide și eficiente pentru schimbul de informații și asistența juridică reciprocă

NATO și strategia de securitate informațională

Centrul de Excelență pentru Apărare Cibernetică NATO

Misiunea centrului este sporirea capacității de cooperare și informare între NATO, inclusiv națiunile membre, și alți parteneri din domeniul apărării cibernetice. Centrul desfășoară activități complexe de cercetare, elaborează lecții învățate și asigură consultanță de specialitate națiunilor membre și partenerilor alianței. O protecție eficientă ar trebui să includă:

- → Cooperare internațională largă

  Dezvoltarea parteneriateor strategice între națiuni și organizații pentru contracararea amenințărilor cibernetice

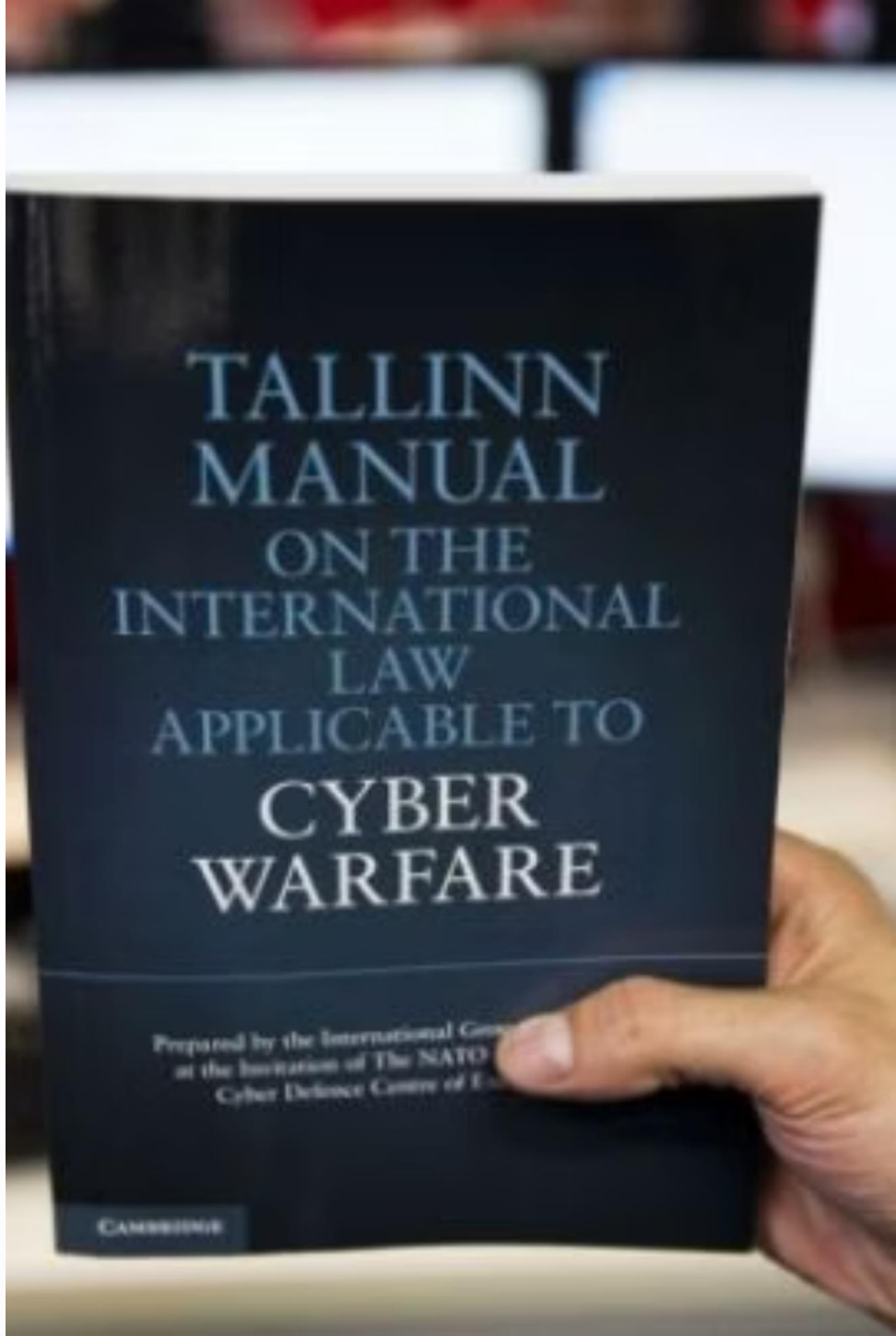
- → Dezvoltarea politicii de coaliție

  Crearea unui cadru politic comun pentru răspunsul coordonat la atacurile cibernetice majore

- → Îmbunătățirea capacităților de apărare

  Consolidarea competențelor tehnice și operaționale pentru operațiuni eficiente în spațiul virtual

Resurse: Vezi publicațiile de la conferința internațională CyCon: "Cyber Conflict: The Next step"



CyCon 2025: ”The Next Step" - Continuitatea în securitatea cibernetică

Tema celei de-a 17-a ediții a CyCon s-a concentrat pe „Următorul pas” în contextul schimbărilor globale rapide. Spațiul cibernetic este un câmp de luptă constant, unde acțiunile ofensive și defensive se estompează, iar conflictul operează sub pragurile tradiționale. Cu actori diverși și amenințări în continuă evoluție, factorii de decizie politică, industria, avocații și tehnologiile trebuie să se adapteze continuu pentru a rămâne în frunte.

Conferința multidisciplinară de patru zile a adus pe scenă peste 100 de experți distinși, inclusiv Jean-Charles Ellermann-Kingombe (Secretar General Adjunct al NATO pentru Inovație, Hibrid și Cibernetică), Dr. Emily Goldman (Senior Cibernetic Strategist al SUA, Agenția Națională de Securitate); Gentlemen Hackers - Mikko Hypponen, Tomi Tuominen cu Thomas Dullien (cunoscut și sub numele de Halvar Flake); Profesorul Ryan Maness (Profesor Asociat de Strategie Cibernetică și Informațională) și Tarah Wheeler (Senior Fellow pentru Politică Cibernetică Globală la Consiliul pentru Relații Externe). Conferința a fost deschisă de președintele Estoniei, Alar Karis.

Domeniile prioritare abordate:

- **Securitatea în transport** - protecția sistemelor de transport inteligente
- **Mediul maritim** - securitatea cibernetică a infrastructurii portuare
- **Lanțul de aprovizionare** - reziliența rețelelor globale de supply chain
- **Tehnologiile autonome** - securitatea vehiculelor și sistemelor autonome

CyCon 2025: ”The Next Step" - Continuitatea în securitatea cibernetică

Tema celei de-a 17-a ediții a CyCon s-a concentrat pe „Următorul pas” în contextul schimbărilor globale rapide. Spațiul cibernetic este un câmp de luptă constant, unde acțiunile ofensive și defensive se estompează, iar conflictul operează sub pragurile tradiționale. Cu actori diverși și amenințări în continuă evoluție, factorii de decizie politică, industria, avocații și tehnologiile trebuie să se adapteze continuu pentru a rămâne în frunte.

Conferința multidisciplinară de patru zile a adus pe scenă peste 100 de experți distinși, inclusiv Jean-Charles Ellermann-Kingombe (Secretar General Adjunct al NATO pentru Inovație, Hibrid și Cibernetică), Dr. Emily Goldman (Senior Cibernetic Strategist al SUA, Agenția Națională de Securitate); Gentlemen Hackers - Mikko Hypponen, Tomi Tuominen cu Thomas Dullien (cunoscut și sub numele de Halvar Flake); Profesorul Ryan Maness (Profesor Asociat de Strategie Cibernetică și Informațională) și Tarah Wheeler (Senior Fellow pentru Politică Cibernetică Globală la Consiliul pentru Relații Externe). Conferința a fost deschisă de președintele Estoniei, Alar Karis.

Temele abordate în cadrul CyCon 2025 au fost structurate pe trei direcții strategice:

- ❑ Strategie: analizează impactul tehnologiilor emergente asupra securității.
- ❑ Drept: explorează modul în care principiile fundamentale ale dreptului internațional se aplică în operațiunile cibernetice, conflictele armate și chiar în contextul spațiului cosmic.
- ❑ Tehnologie: oferă un cadru de discuții tehnice avansate, de la exploatarea vulnerabilităților și dezvoltarea de soluții inovatoare, până la antrenamente tehnice specializate pentru profesioniștii din domeniu.

Forumul “EaPCyberWomen”

Forumul Eastern Partnership Women in Cyber este o inițiativă strategică menită să combată lipsa alarmantă de diversitate în acest sector, prin împuternicirea și perfecționarea profesionistelor din domeniu. Evenimentul, organizat în Moldova, la 6 și 7 martie 2025 a reunit lideri din industrie, cadre academice, specialiști și aspiranți din țările Parteneriatului Estic și partenerii UE, pentru a construi și dezvolta un ecosistem solid care sprijină implicarea și avansarea femeilor în securitatea cibernetică.

Peisajul securității cibernetice din regiunea Parteneriatului Estic, precum și la nivel global, evoluează rapid, aducând provocări și amenințări din ce în ce mai complexe și interconectate. Creșterea dependenței de tehnologiile informaționale și serviciile digitale, alături de numărul tot mai mare de incidente, vulnerabilități și amenințări, determină o expansiune rapidă a sectorului securității cibernetice, generând o cerere constantă de profesioniști calificați.

Tematicile prioritare abordate:

- Securitate internațională, cu accent pe provocările globale și regionale în domeniul securității cibernetice
- Schimb de cunoștințe, competențe și bune practici, mentorat și dezvoltare profesională
- Personalități inspiraționale și exemple de impact din sectorul securității cibernetice
- Reducerea deficitului de forță de muncă în securitate cibernetică printr-o mai mare incluziune a femeilor

Cadrul european de securitate cibernetică

Strategii și instrumente europene

Strategia societății informaționale

"Dialog, Parteneriat și Extinderea Capacității" - oferă o imagine de ansamblu asupra stării amenințărilor la securitatea societății informaționale și determină măsuri suplimentare pentru asigurarea securității rețelelor și informațiilor.

Programul de la Stockholm

"O Europă deschisă și sigură" - prevede măsuri suplimentare pentru îmbunătățirea luptei împotriva criminalității informatice, focalizându-se pe protecția cetățenilor europeni.

ENISA - Centrul de expertiză

Agenția UE pentru Securitatea Rețelelor și Informațiilor - centru de expertiză pentru securitatea cibernetică în Europa, asistând UE și statele membre în prevenirea, detectarea și eliminarea problemelor de securitate informațională.

Aceste instrumente creează un ecosistem integrat de securitate cibernetică la nivel european, oferind soluții practice pentru instituțiile UE și sectoarele public și privat din țările membre.

ENISA și protecția datelor în era GDPR

Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) a publicat un raport comprehensiv despre integrarea tehnologiilor de securitate cibernetică cu principiile Regulamentului General privind Protecția Datelor (GDPR) în contextul partajării datelor cu caracter personal.

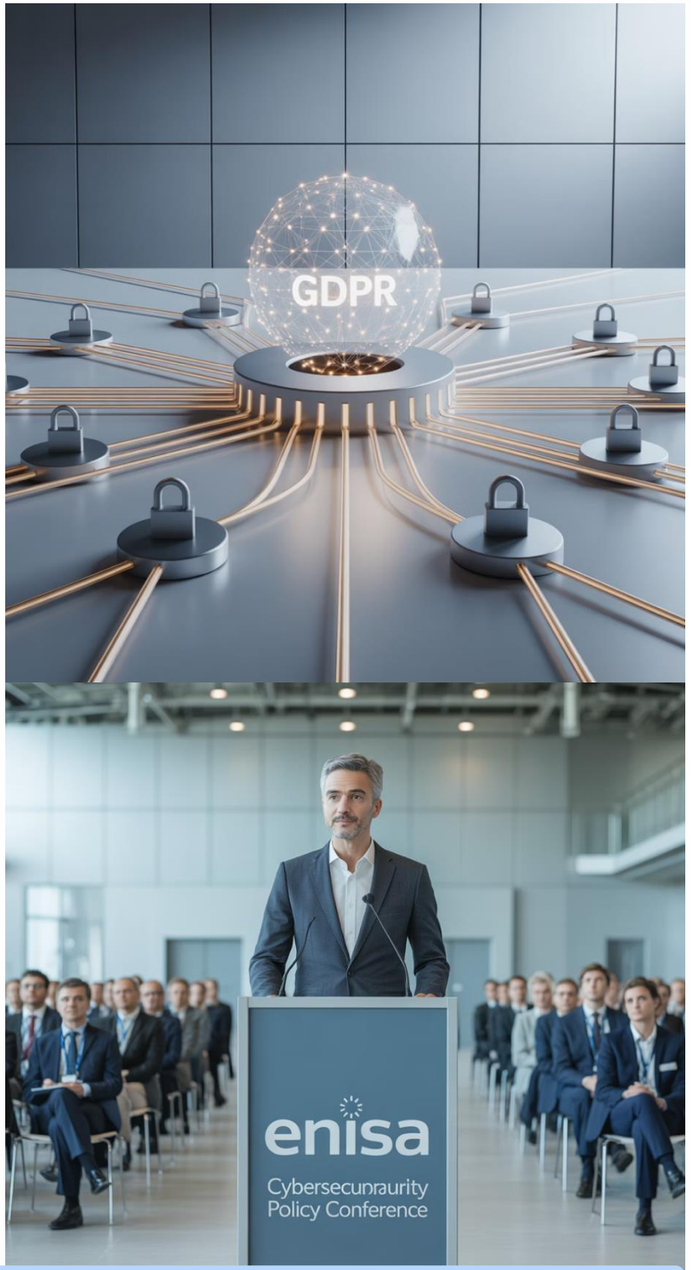
Aspecte-cheie analizate:

- **Procesarea datelor** - modalități de tratare a informațiilor în timpul partajării
- **Canale secundare** - securizarea tranzitului prin entități intermediare
- **Drepturi fundamentale** - implementarea dreptului la ștergere și rectificare
- **Soluții practice** - abordări eficiente pentru factori de decizie și practicieni

Prima conferință de politică ENISA-CE

Obiectivul central: sprijinirea dezvoltării continue a politicilor pentru atingerea unui nivel comun ridicat de securitate cibernetică, incluzând implementarea provisiunilor NIS 2 în întreaga UE.

Evenimentul a fost menit să abordeze provocările în implementarea noilor prevederi ale NIS 2 în întreaga UE (https://digital-strategy.ec.europa.eu/ro/policies/nis2-directive). De asemenea, a arătat cum să faciliteze procesul de implementare, precum și să discute despre noile evoluții în cadrul politicii UE de securitate cibernetică. Experții au discutat despre o abordare comună a cadrului legislativ actual al UE și au făcut schimb de opinii.



Link util: NIS 2 Directive

Evoluția securității cibernetice în Republica Moldova

CERT-GOV-MD - Primul pas strategic

CENTRUL DE TELECOMUNICAȚII SPECIALE

CSC Centrul pentru Securitatea Cibernetică

Centrul pentru Securitatea Cibernetică - CERT-GOV-MD a reprezentat prima inițiativă structurată pentru abordarea sistemică a securității informaționale în Republica Moldova.

Misiunea fundamentală:

- Asistența beneficiarilor în utilizarea securizată a sistemelor IT governamentale
- Implementarea măsurilor proactive și reactive pentru reducerea riscurilor
- Acordarea asistenței specializate în gestionarea incidentelor de securitate
- Examinarea și analiza incidentelor raportate de cetățeni și instituții

Centrul examina incidentele apărute în rețelele naționale raportate atât de către cetățeni și instituții din Republica Moldova, cât și de către parteneri internaționali, contribuind la dezvoltarea unei viziuni comprehensive asupra peisajului amenințărilor cibernetice la nivel național.

Programul e-Transformare și securitatea cibernetică

În 2010, Republica Moldova a lansat procesul ambițios de guvernare electronică prin programul strategic **e-Transformare**, oferind o viziune unificată de modernizare și îmbunătățire a accesului publicului la serviciile guvernamentale prin tehnologiile informaționale.

1

2010 - Lansarea e-Transformare

Inițierea programului strategic de digitalizare a serviciilor publice cu focus pe accesibilitatea și eficiența pentru cetățeni

2

Provocări de securitate

Dezvoltarea rapidă a sistemelor nu a inclus inițial controale suficiente pentru asigurarea securității cibernetice globale

3

Răspunsul institutional

Crearea CERT-GOV-MD în cadrul Întreprinderii de Stat "Centrul de telecomunicații speciale" ca răspuns la necesitățile de securitate

> Asigurarea informațională - încrederea în securitatea, integritatea și disponibilitatea sistemelor informatice - este esențială pentru succesul transformării digitale. O dezvoltare logică include implementarea de sisteme noi împreună cu măsuri adecvate de protecție.

Reorganizarea instituțională - STISC

Transformarea strategică din 2018

Din 18 mai 2018, Întreprinderea de Stat „Centrul de Telecomunicații Speciale" se reorganizează prin transformare în **Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică" (STISC).**

Mandatul extins al STISC:

- **Administrarea infrastructurii IT** - menținerea și dezvoltarea sistemelor tehnologice guvernamentale
- **Telecomunicații speciale** - gestionarea rețelei de comunicații speciale
- **Sisteme informaționale de stat** - administrarea platformelor critice naționale
- **Infrastructura PKI** - gestionarea sistemului unic de chei publice guvernamentale
- **Politici de securitate** - implementarea strategiilor naționale de securitate cibernetică

Această reorganizare a marcat o evoluție semnificativă în abordarea securității cibernetice naționale, integrând responsabilitățile tehnice cu cele de politică publică într-o singură instituție specializată.

Activitatea contemporană a STISC

Site-ul oficial al STISC furnizează informații actuale din domeniul securității cibernetice, reflectând angajamentul instituției în informarea publică și transparența activității.

Evenimente și inițiative recente:

- **Forumul "Her CyberTracks"** - Muntenegru, focalizat pe participarea femeilor în politicile de securitate cibernetică
- **Cooperarea regională** - cu țări din Balcanii de Vest și Europa de Est
- **Monitorizarea amenințărilor** - raportarea tendințelor în atacurile cibernetice

Statistici alarmante actuale:

- Tentativă de atac cibernetic uriaș cu o zi înaintea alegerilor parlamentare în Republica Moldova. STISC a confirmat că peste 16 milioane de tentative de atac cibernetic au avut loc în noaptea de sâmbătă spre duminică.
- Mii de routere Wi-Fi din locuințele cetățenilor au fost compromise În dimineața zilei de 24 septembrie. Scopul atacatorilor ar fi utilizarea rețelelor infectate pentru a lansa, în ziua alegerilor, atacuri asupra serverelor și infrastructurii CEC.

Ziua Siguranței pe Internet - responsabilitate și protecție online

Ziua Siguranței pe Internet, eveniment global celebrat anual în a doua zi de marți a lunii februarie, dedicat promovării unui mediu online mai sigur și mai responsabil, în special pentru copii și tineri. Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) îndeamnă cetățenii, instituțiile, mediul de afaceri și societatea civilă să se alăture campaniei internaționale „Împreună pentru un Internet mai bun”

Pentru un plus de siguranță digitală, țineți cont de următoarele măsuri:

- Nu distribuiți datele personale în mediul online;
- Evitați accesarea linkurilor și atașamentelor suspecte primite prin e-mail, SMS sau aplicații de mesagerie;
- Actualizați constant browserul și aplicațiile utilizate;
- Folosiți parole puternice, unice, și activați autentificarea în doi pași;
- Verificați setările de confidențialitate ale conturilor de pe rețelele sociale;
- Evitați rețelele Wi-Fi publice nesecurizate;
- Raportați conținutul sau comportamentele suspecte întâlnite online.

Exercițiul internațional de combatere a fraudelor online

Moldova a marcat Luna Europeană a Securității Cibernetice 2025 prin lansarea unei campanii naționale menite să abordeze una dintre cele mai alarmante provocări din ultimii ani: frauda online.

Desfășurată sub motto-ul „Stop investițiilor false!”, inițiativa răspunde la creșterea bruscă a infracțiunilor financiare comise în sfera digitală, numărul cazurilor în 2025 aproape dublându-se față de 2023. Campania, care include o varietate de videoclipuri, mesaje audio, materiale tipărite și conținut pentru rețelele sociale, are ca scop sensibilizarea publicului, încurajarea vigilenței și promovarea unor comportamente online mai sigure în rândul cetățenilor.

Dark Web

Tehnici avansate de investigare și monitorizare a activităților criminale în rețelele obscure

Criptomonede

Metodologii de urmărire a tranzacțiilor și identificarea fluxurilor financiare ilicite

Fraude online

Strategii de detectare și contracarare a schemelor de fraudă în plățile electronice

Scopul companiilor, training-urilor regionale este de a a îmbunătăți cunoștințele participanților cu privire la cele mai comune forme de atacuri cibernetice, consolidând capacitățile naționale de răspuns la amenințările digitale contemporane.

Serviciul de Informații și Securitate - dimensiunea internațională

Securitatea Republicii Moldova constituie o componentă integrală a securității mondiale. În epoca globalizării contemporane, emergența amenințărilor asimetrice necesită consolidarea parteneriateelor durabile în cadrul comunității informative internaționale pentru diminuarea riscurilor care pun în pericol securitatea națională și regională.

Evoluția cooperării după 1991:

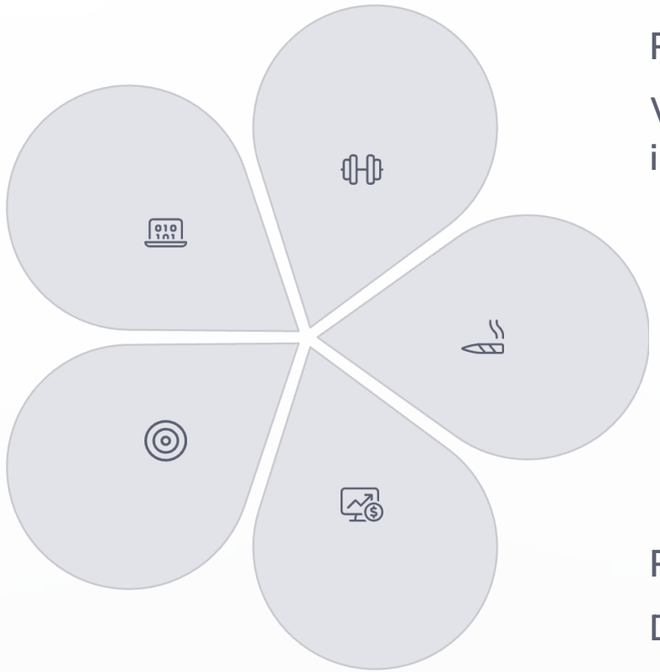
De la fondarea instituției, raporturile de cooperare ale SIS au cunoscut o dinamică pozitivă, manifestându-se prin diverse forme de colaborare: schimb de informații și expertiză, participare la evenimente de profil și realizarea de operațiuni comune cu partenerii externi.

Schimb informațional

Transfer rapid de informații despre amenințări și vulnerabilități

Partajarea experienței

Valorificarea cunoștințelor și bunelor practici internaționale



Operațiuni comune

Colaborări operative pentru contracararea amenințărilor transfrontaliere

Parteneriate strategice

Relații pe termen lung cu serviciile de securitate partenere

Programe de formare

Dezvoltarea competențelor prin instruiri specializate

Integrarea europeană și securitatea informațională

În contextul politicii de integrare europeană a Republicii Moldova, Serviciul de Informații și Securitate își propune ca imperativ strategic aderarea la platformele informative regionale și stabilirea de relații bilaterale și multilaterale robuste cu instituțiile de profil de pe arena internațională.

Obiectivul strategic fundamental:

> Realizarea intereselor fundamentale de securitate națională și implicarea activă a SIS în crearea unui climat adecvat de securitate regională și europeană, având ca finalitate promovarea imaginii Republicii Moldova nu doar în calitate de **consumator**, dar și **generator de securitate**.

Platforme regionale

Aderarea la mecanismele de cooperare în securitate la nivel regional european

Relații bilaterale

Dezvoltarea parteneriateelor directe cu serviciile de securitate europene

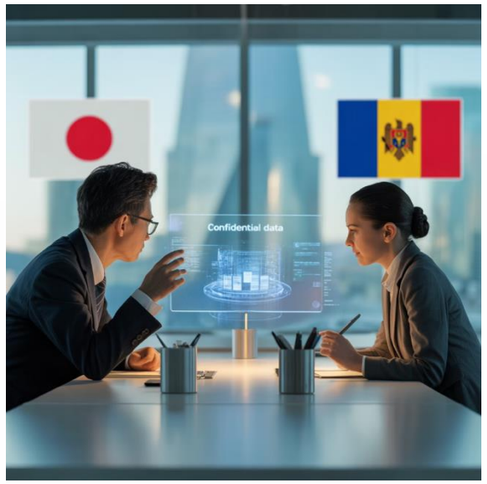
Cooperare multilaterală

Participarea activă în formate multilaterale de securitate internațională

Cooperarea moldo-japoneză în securitatea cibernetică

În iunie 2022, Viceprim-ministrul pentru digitalizare și directorul STISC au avut o întrevedere strategică la Chișinău cu directorul oficiului Agenției Japoneze pentru Cooperare Internațională (JICA) în Ucraina, Satoshi Sugimoto, în cadrul unei vizite de lucru focalizate pe oportunitățile de finanțare a proiectelor de dezvoltare.

Domeniile prioritare de cooperare:



Consolidarea rezilienței STISC

- Fortificarea sistemelor informaționale guvernamentale
- Dezvoltarea capacităților de răspuns la incidente
- Modernizarea infrastructurii de securitate

Programe de instruire 2023

- Schimbul de experiențe și cunoștințe
- Partajarea bunelor practici internaționale
- Dezvoltarea competențelor profesionale

Rezultat: Reprezentanții JICA au salutat intenția autorităților moldovenești de continuare a cooperării și și-au exprimat disponibilitatea pentru extinderea domeniilor de interes și crearea de parteneriate de succes.

Securitatea sistemului financiar global

În economia mondială contemporană, tranzacțiile internaționale sunt utilizate în mod fraudulos ca componentă de bază a spălării banilor și finanțării terorismului. Sistemul financiar global, transformat dintr-o componentă a pieței într-un factor independent al economiei globale, facilitează fluxurile bănești masive provenite din economia subterană.

Volumul fraudelor transnaționale

Creșterea continuă a dimensiunilor criminalității economice organizate la nivel internațional

Circulația capitalului suspect

Intensificarea fluxurilor bănești de origine suspectă prin canale financiare legitime

Tehnologii alternative

Utilizarea pe scară largă a metodelor de transfer care evită supravegherea tradițională

Infiltrarea sectorului legal

Integrarea capitalurilor ilicite în economia legală prin diverse mecanisme sofisticate

> Avansarea circulației informației, capitalului, persoanelor, bunurilor și serviciilor necesită modificarea concepției tradiționale și a atitudinii față de crimele transnaționale.

Implicarea societății civile în securitatea cibernetică

Asigurarea măsurilor de prevenire a atacurilor cibernetice și limitarea efectelor acestora sunt absolut necesare, dar este crucială și implicarea activă a societății civile, care trebuie să conștientizeze necesitatea colaborării cu autoritățile pe acest palier strategic.

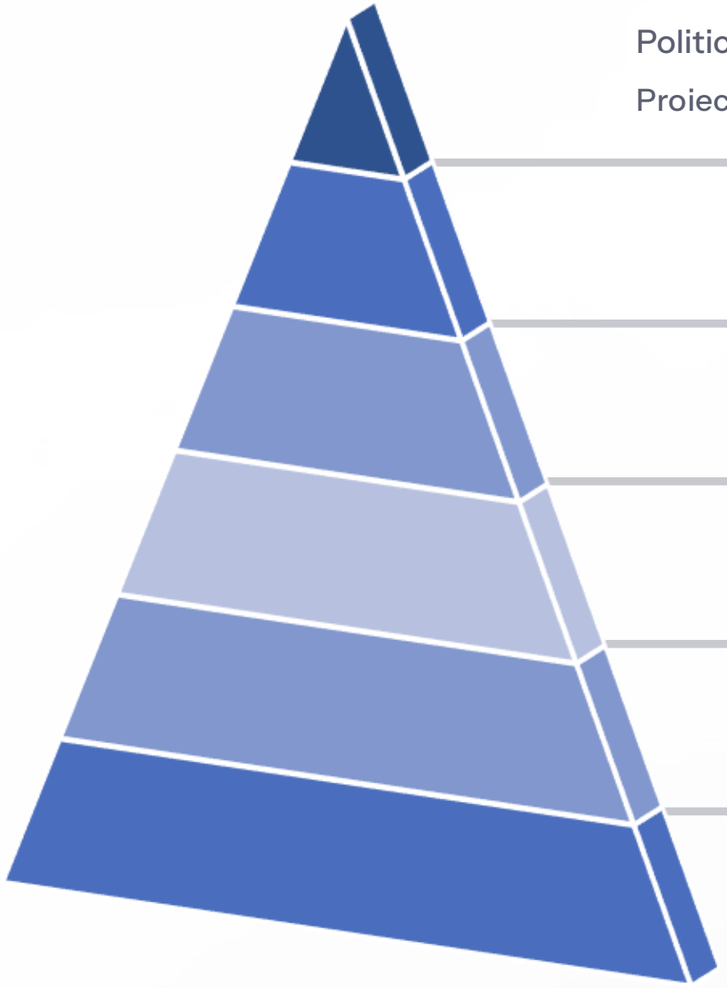
Elementele cheie ale participării civile:

- **Conștientizarea riscurilor** - educarea publicului despre amenințările cibernetice
- **Raportarea incidentelor** - încurajarea cetățenilor să raporteze activități suspecte
- **Adoptarea bunelor practici** - implementarea măsurilor de securitate personale
- **Cooperarea cu autoritățile** - sprijinirea investigațiilor și măsurilor preventive

Această abordare colaborativă creează un ecosistem de securitate comprehensiv în care responsabilitatea este distribuită între instituțiile statului și cetățeni, maximizând eficiența măsurilor de protecție.

Concluzii - Necesitatea unui cadru legal matur

În actualul context complex de securitate, adoptarea unui cadru legal comprehensiv care să sprijine dezvoltarea capacităților elementelor de securitate ale statului pentru a face față amenințărilor cibernetice reprezintă o necesitate imperioasă pentru orice națiune și un pas fundamental în dezvoltarea unui sistem matur de securitate cibernetică.



Politici și strategii

Proiectarea de politici și strategii de securitate cibernetică adaptate la realitățile naționale

Cultura de securitate

Creșterea culturii de securitate cibernetică la nivelul societății civile prin educație și sensibilizare

Competențe cibernetice

Dezvoltarea competențelor atât la nivelul utilizatorilor, cât și al managerilor din diferite sectoare

Cadru legal eficient

Crearea unui cadru legal și a unor acte normative eficiente și adaptate amenințărilor contemporane

Managementul riscului

Implementarea sistemelor organizaționale pentru managementul proactiv al riscurilor cibernetice

Standarde tehnologice

Impunerea de standarde și implementarea de tehnologii avansate pentru protecția sistemelor

Concluzii - Etapele dezvoltării sistemului matur de securitate

Atingerea obiectivelor strategice permite unei entități să își auto-evalueze capabilitățile de securitate cibernetică și să determine nivelul de maturitate al sistemului său de securitate.

Procesul de maturizare - de la incipiență la excelență

Constituirea unui sistem matur de securitate implică o evoluție treptată de la prima fază, caracterizată prin absența capabilităților de securitate cibernetică, până la etapa finală de maturitate completă.

1 Faza inițială

Absența mecanismelor de securitate cibernetică și a conștientizării riscurilor

2 Dezvoltarea graduală

Implementarea primelor măsuri de protecție și formarea competențelor de bază

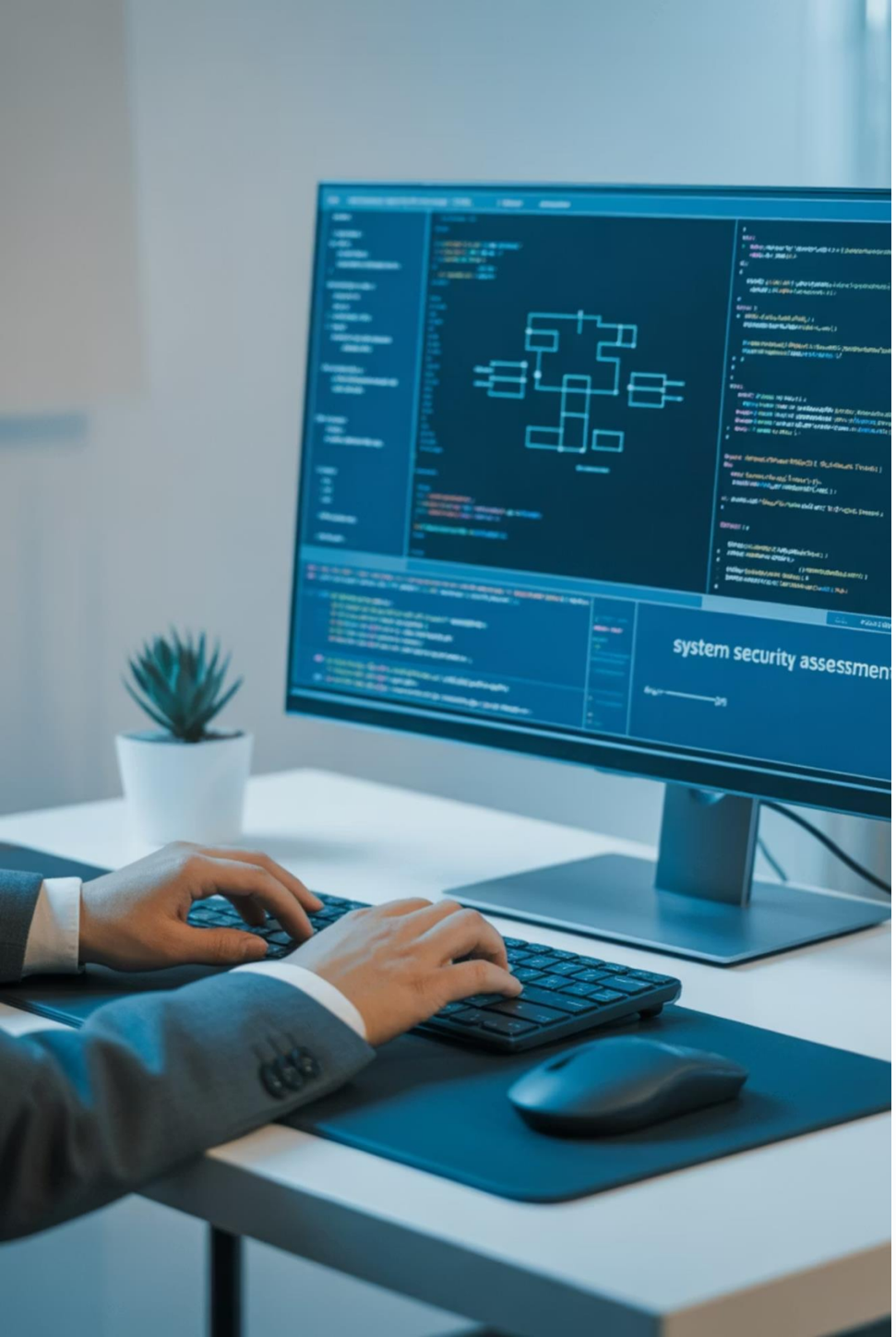
3 Consolidarea capacităților

Dezvoltarea procedurilor și mecanismelor specializate de răspuns

4 Maturitatea completă

Mecanisme clare de gestionare, adaptare strategică și realocare de resurse

Schimburile de informații, instruirile comune concentrate pe îmbunătățirea abilităților profesionale de detectare și investigare a criminalității cibernetice prin utilizarea metodelor și tehnicilor conforme legislației internaționale pot spori doar printr-o **colaborare, comunicare și conlucrare eficientă**.



Sarcini de autoevaluare

Acorduri de cooperare internațională

Identificați acordurile existente la nivel internațional pentru îmbunătățirea capacității de răspuns în cazul atacurilor cibernetice majore. Analizați eficiența și aplicabilitatea acestora în contextul Republicii Moldova.

Interese naționale în cooperarea internațională

Determinați și evaluați interesele naționale de securitate cibernetică în formatele de cooperare internațională la care Republica Moldova este parte sau aspiră să devină membru.

Programe internaționale de securitate

Evaluați participarea și activitatea Republicii Moldova la programele internaționale care vizează domeniul securității cibernetice, identificând oportunitățile de îmbunătățire a implicării.

Aceste sarcini vor fi evaluate pe baza analizei critice, utilizării surselor relevante și formulării de recomandări practice pentru îmbunătățirea cooperării internaționale în domeniul securității informaționale.

Teme pentru lucrul individual

Provocări actuale în securitatea cibernetică

Analizați impactul și contribuția Republicii Moldova în abordarea provocărilor contemporane din domeniul securității cibernetice la nivel regional și internațional

Importanța cooperării informaționale

Evaluați rolul critic al cooperării în aria securității informaționale/cibernetice pentru eficientizarea răspunsului la amenințările transfrontaliere

Bune practici de prevenire

Identificați și analizați bunele practici pentru prevenirea și limitarea efectelor atacurilor cibernetice la nivelul instituțiilor publice din Republica Moldova

Mecanisme de cooperare

Studiați mecanismele de cooperare la nivel european și internațional, evaluând posibilitățile de implementare și adaptare la contextul național

Dezvoltarea cooperării

Propuneți strategii pentru dezvoltarea cooperării naționale și internaționale în domeniul securității informaționale, incluzând aspecte juridice, tehnice și instituționale

Bibliografie și resurse

Surse internaționale:

1. 17th International Conference on Cyber Conflict: The Next Step, CCDCOE Publications. 2025.
2. https://ccdcoe.org/cycon/
2. ENISA - Tehnici de securitate cibernetică pentru protecția datelor: https://www.enisa.europa.eu/publications/engineering-personal-data-sharing
3. ENISA - Prima conferință de politică în securitatea cibernetică: https://www.enisa.europa.eu/news/supporting-policy-developments
4. Parteneriatele NATO și Republica Moldova în fața noilor amenințări. Chișinău, 2014

Resurse naționale și regionale:

1. Democrația sub asediu. Provocări la adresa securității naționale și contracararea amenințărilor hibride în Republica Moldova, 2025
2. Cooperare pentru securitate cibernetică: https://cybersecuritytrends.ro/cooperare-pentru-securitate-cibernetica/
3. Conferința "Securitatea Cibernetică în RM": http://cert.gov.md/news/noutati/article//conferinta.html
4. Problematica securității cibernetice în organizațiile internaționale: https://www.mae.ro/node/28369
5. Programul de Securitate Cibernetică RM: http://www.mtic.gov.md/ro/projects/programul-de-securitate-cibernetica
6. Protejarea spațiului informațional. https://pisa.md/wp-content/uploads/2025/01/Protejarea-spatiului-informational_STUDIU.pdf

Studii academice:

1. Мазуров В. Кибертерроризм: понятие, проблемы противодействия. Доклады ТУСУРа, 2010
2. Смирнов А. Обеспечение информационной безопасности в условиях виртуализации общества. Москва: ЮНИТИ-ДАНА, 2011
3. Tielidze G., Bagge D., Spinu N. Regional Cyber Security. Per Concordiam, Vol. 5, 2014