

Dezvoltarea cooperării internationale în domeniul securității informaționale

**Autor: Tatiana Busuncian
Dr., conferențiar universitar**

Chișinău 2025

Conținuturi; Obiective de referință; termeni-cheie

Conținuturi:

1. Dezvoltarea cooperării internaționale în domeniul securității informaționale;
2. Principalele direcții de colaborare în domeniul securității informaționale;
3. Asigurarea securității informaționale, inclusiv în Republica Moldova.

Obiective de referință:

- să identifice căile de colaborare internațională 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 internațională la care Republica Moldova este parte;
- să evalueze activitatea la programe internaționale care vizează domeniul securității informaționale.

Termeni-cheie: *Cooperare, direcții de colaborare, acorduri de cooperare, interese naționale.*



Începând cu anii 70 - perioada
prezumtivă de apariție a criminalității
informatică.



Criminalitatea informatică este
orice infracțiune care poate fi comisă prin
intermediul:

- a). unui sistem informatic sau de rețea;
- b). ca parte a unui sistem informatic sau de rețea;
- c). sau împotriva unui sistem informatic sau de rețea.

ȚINTE

organizațiile internaționale

autoritățile înalte ale puterii executive și legislative

instituțiile blocului economic

universitățile anumitor state

organizații sociale

sistemul bancar

Obiecte ale infrastructurii critice

CATEGORIILE SURSELOR CRIMINALITĂȚII INFORMAȚIONALE

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

Hacktiviștii. 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

Teroriștii

Se presupune că termenul *terorismul cibernetic* a apărut în vocabularul IT în anul 1997.



Agentul special FBI Mark Pollitt a definit acest tip de terorism ca “atacul premeditat, motivat politic împotriva informației, sistemelor informatice, programelor informatice și datelor, rezultând în violența împotriva țăintelor noncombatante, de către grupări sub-nationale sau agenți clandestini”.

- 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.

DEZVOLTAREA COOPERĂRII INTERNAȚIONALE ÎN DOMENIUL SECURITĂȚII INFORMAȚIONALE

- Societatea actuală este caracterizată de cunoaștere și continuă schimbare. Asistăm astăzi la o lume globală, complexă, dinamică, fapt determinat de mutațiile ce au loc pe fondul procesului de globalizare și al dependenței informaționale.
- Evoluția exponențială a mediului informațional și valențele strategice dobândite de țările dezvoltate au generat riscuri și vulnerabilități, ce sunt sau pot fi exploatare de entități răuvoitoare în scopul săvârșirii de infracțiuni, acte de spionaj, ce pun în pericol atât indivizii, cât și societatea.
- În acest context, provocările în domeniul securității informaționale sunt tot mai complexe și mai variate, fiecare stat având obligativitatea de a identifica și dispune măsuri de dezvoltare a unor mecanisme eficiente de reziliență și răspuns la amenințările mediului virtual.

DEZVOLTAREA COOPERĂRII INTERNAȚIONALE ÎN DOMENIUL SECURITĂȚII INFORMAȚIONALE

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



DEZVOLTAREA COOPERĂRII INTERNAȚIONALE ÎN DOMENIUL SECURITĂȚII INFORMAȚIONALE

Existența la nivelul fiecărui stat a unui cadru normativ în domeniul securității informaționale este necesară, în condițiile în care nivelul amenințării la nivel internațional este în continuă creștere. În evaluarea nivelului amenințării informaționale avem în vedere, pe de o parte, riscurile generate de interesul anumitor entități statale și criminale de a compromite infrastructuri informaționale/cibernetice și, pe de altă parte, vulnerabilitățile sistemelor informatice, fie software, fie de natură umană (pe fondul precarității culturii de securitate cibernetică).



DEZVOLTAREA COOPERĂRII INTERNAȚIONALE ÎN DOMENIUL SECURITĂȚII INFORMAȚIONALE



Opiniile pe marginea necesității unei legi în domeniul securității informaționale variază, îmbrăcând nuanțe diverse, în tonalități diferite. De exemplu, în registru negativ sunt relevante temerile că aplicarea unui astfel de act normativ ar fi de natură să încalce intimitatea personală și că, în esență, ar conduce la o constrângere din partea autorităților competente, înțeleasă în termeni de limitare a exercițiului unor drepturi și libertăți (mai exact limitarea dreptului la viață intimă, familială, la secretul corespondenței, libertatea de exprimare).

DEZVOLTAREA COOPERĂRII INTERNAȚIONALE ÎN DOMENIUL SECURITĂȚII INFORMAȚIONALE

Calculatorul oricărei persoane fizice, care nu are un minimum de cunoștințe în domeniul securității informaționale/cibernetice, poate fi ținta unui atac sau poate fi folosit pentru un atac cibernetic, fără ca măcar să știe acest lucru.

Educarea societății civile în sensul creșterii culturii de securitate, dar și creșterea încrederii între stat și societatea civilă sunt puncte esențiale de atins în obținerea unui deziderat privind spațiul cibernetic. În acest sens, modernizarea programelor de studii existente la nivelul învățământului gimnazial, dar și pregătirea personalului din administrația publică și formarea unor magistrați cu competențe în domeniul securității informaționale ar putea să soluționeze câteva din problemele pe care le regăsim la nivelul societății civile.



CLASIFICAREA CRIMINALITĂȚII INFORMATICE

I. Clasificarea ONU



- Crime impotriva sistemelor informatice

- Crime comise pe sau prin intermediul calculatoarelor

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

Crime împotriva sistemelor informatice



Crime comise pe sau prin intermediul calculatoarelor



Infracțiuni referitoare la conținut



Infracțiuni referitoare la atingerile aduse
proprietății intelectuale și 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

Fiecare stat utilizează un set de instrumente, politici, principii, măsuri de siguranță, abordări de gestionare a riscurilor, acțiuni, formarea, experiența, asigurare și tehnologii, care pot fi utilizate pentru protejarea spațiului informatic, pentru resursele organizației și a utilizatorului.



CONVENȚIA PRIVIND CRIMINALITATEA INFORMATICĂ

Sarcinile principale:

1) adoptarea unei legislații adecvate, precum și prin îmbunătățirea cooperării internaționale, referitor la infracțiuni și dispoziții relevante în domeniul criminalității informatice și prevederilor în domeniul criminalității cibernetice;

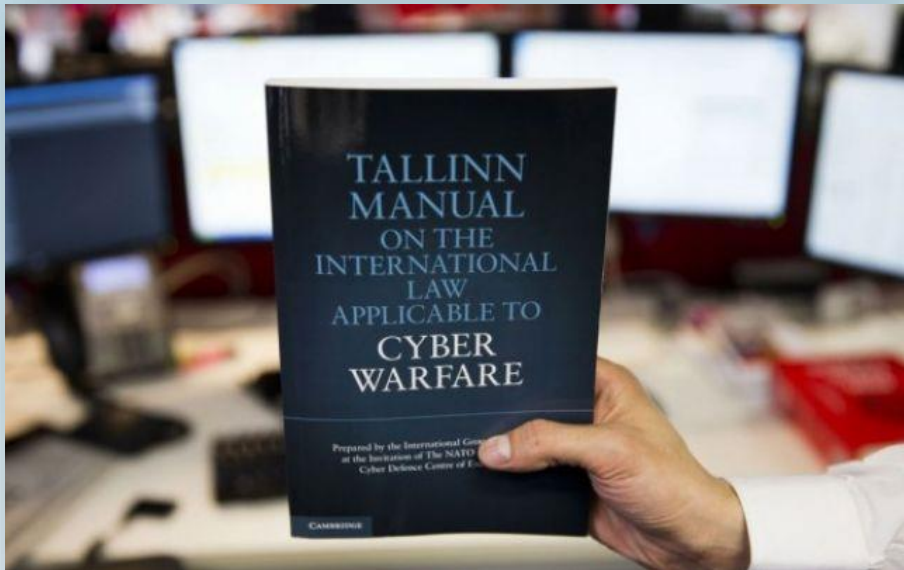
2) stabilirea competențelor și procedurilor necesare pentru investigarea și urmărirea penală pentru aceste infracțiuni, precum și pentru alte infracțiuni săvârșite prin intermediul sistemelor informatice;

3) colectarea probelor în format electronic;

4) elaborarea mecanismelor de cooperare internațională rapide și eficiente.

NATO și SECURITATEA INFORMAȚIONALĂ

Centrul de Excelență pentru Apărare Cibernetică NATO a cărei misiune este sporirea capacității de cooperare și informare între NATO, incluzând și națiunile membre, și alți parteneri din domeniul apărării cibernetice. De asemenea, Centrul desfășoară activități de cercetare, elaborează lecții învățate și asigură consultanță de specialitate națiunilor membre și partenerilor alianței



O protecție eficientă a spațiului virtual ar trebui să includă :

- cooperare internațională largă;
- dezvoltarea politicii de coaliție;
- îmbunătățirea capacităților de apărare pentru operațiuni în spațiul virtual.

Vezi publicații de la conferința internațională a 14: Cyber Conflict: Keep Moving

Asigurarea securității cibernetice în cadrul Uniunii Europene

STRATEGIA DE SECURITATE A SOCIETĂȚII INFORMAȚIONALE "DIALOG, PARTENERIAT ȘI EXTINDEREA CAPACITĂȚII,,

Această strategie oferă o imagine de ansamblu a stării actuale a amenințărilor la adresa securității societății informaționale și determină măsuri suplimentare pentru a asigura securitate rețelelor și a informațiilor.

**PROGRAMUL DE LA STOCKHOLM – O EUROPĂ DESCHISĂ ȘI SIGURĂ
ÎN SERVICIUL CETĂȚENILOR ȘI PENTRU PROTECȚIA ACESTORA -**
prevede măsuri suplimentare pentru îmbunătățirea luptei împotriva criminalității informatice.

**AGENȚIA UNIUNII EUROPENE PENTRU SECURITATEA REȚELELOR ȘI
A INFORMAȚIILOR (ENISA)** - este un centru de expertiză pentru securitatea cibernetică în Europa, ajută UE și statele membre să fie mai bine echipate și pregătite pentru a preveni, detecta și elimina problemele legate de securitatea informațiilor. Oferă sfaturi și soluții practice pentru instituțiile UE și pentru sectorul public și privat din țările membre.

ENISA a publicat un raport cu referire la tehnicile de securitate cibernetică pentru protecția datelor

Agencia Uniunii Europene pentru Securitate Cibernetică (ENISA) a publicat un raport despre modul în care tehnologiile și tehnicile de securitate cibernetică pot sprijini implementarea principiilor Regulamentului general privind protecția datelor (GDPR) atunci când partajează date cu caracter personal. Documentul prezintă o analiză a modului în care datele sunt tratate atunci când partajarea face parte dintr-un alt proces sau serviciu. Acesta este cazul când datele trebuie să treacă printr-un canal sau o entitate secundară înainte de a ajunge la destinatarul final. La fel, raportul se concentrează pe diferitele provocări și posibile soluții, spre exemplu dreptul la ștergere și dreptul la rectificare la partajarea datelor. Vizând factorii de decizie politică și practicienii în protecția datelor, raportul oferă o privire de ansamblu asupra diferitelor aspecte ale modului de abordare a partajării datelor cu caracter personal într-un mod eficient.

Agencia Uniunii Europene pentru Securitate Cibernetică (ENISA) a organizat prima conferință de politică în domeniul securității cibernetică împreună cu Comisia Europeană pentru a discuta evoluția cadrului politicilor de securitate cibernetică a UE. Obiectivul central al reuniunii a fost suportul continuu în dezvoltarea politicilor pentru a atinge un nivel comun ridicat de securitate cibernetică.

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.

SECURITATEA CIBERNETICĂ în REPUBLICA MOLDOVA



Pe site-ul „Serviciul Tehnologia Informației și Securitate Cibernetică” găsiți noutăți de ultimă oră din domeniul securității cibernetice.

Spre exemplu: forumul regional ”Her CyberTracks” care a avut loc în Muntenegru. Beneficiare ale forumului au fost femeile implicate în activități naționale și internaționale, procesele și negocierile privind politica de securitate cibernetică din Republica Moldova, Albania, Bosnia și Herțegovina, Georgia, Muntenegru, Macedonia de Nord, Serbia și Ucraina.

Noutăți din domeniul securității cibernetice:
Atacurile de tip phishing pe Messenger generează peste 100.000 de mesaje săptămânale;
Atacul de phishing Microsoft Teams vizează rețelele corporative;

IBM: 90% dintre atacurile cibernetice încep cu phishing prin e-mail și altele.



Asigurarea securității în Sistemul financiar global

În economia mondială sunt utilizate, în mod fraudulos, tranzacțiile internaționale drept componentă de bază a spălării banilor și a finanțării terorismului. Sistemul financiar global, transformat din parte componentă a pieței într-un factor independent al economiei globale, susține fluxurile bănești masive, provenite din economia tenebră.

Volumul fraudelor economice transnaționale se conturează tot mai mult. Circulația capitalului, inclusiv fluxurile bănești de origine suspectă, iau amploare. Sunt pe larg utilizate tehnologiile informaționale alternative pentru transfer, care, în majoritatea cazurilor, privează de informație organele de supraveghere.

Este de menționat faptul că o parte substanțială a capitalurilor provenite din activități ilicite ajung în sectorul economic legal. Avansarea circulației informației, capitalului, persoanelor, bunurilor și serviciilor, necesită modificarea concepției tradiționale și a atitudinii față de crimele transnaționale.

Asigurarea unor măsuri de prevenire a atacurilor cibernetice și de limitare a efectelor acestora sunt absolut necesare, dar este nevoie și de implicarea societății civile, care trebuie să conștientizeze necesitatea colaborării cu autoritățile pe acest palier.



ConcluziiI

În actualul context de securitate, adoptarea unui cadru legal care să sprijine dezvoltarea capacităților elementelor de securitate ale statului, astfel încât să facă față amenințărilor cibernetice este un lucru necesar pentru orice stat și un pas important în dezvoltarea unui sistem matur de securitate cibernetică.

Deținerea unui sistem matur de securitate cibernetică reprezintă, de altfel, scopul fiecărui stat, pentru realizarea lui fiind necesară îndeplinirea mai multor obiective, precum: proiectarea unor politici și a unei strategii de securitate cibernetică; creșterea culturii de securitate cibernetică la nivelul societății civile; dezvoltarea unor competențe cibernetice atât la nivelul utilizatorilor, cât și la nivelul managerilor; crearea unui cadru legal și a unor acte normative eficiente; managementul riscului prin organizare; impunerea de standarde și tehnologie.

Sarcini de autoevaluare

- Identificați acorduri de cooperare la nivel internațional pentru îmbunătățirea capacității de răspuns în cazul unor atacuri cibernetice majore;
- Determinați interesele naționale de securitate cibernetică în formatele de cooperare internațională la care Republica Moldova este parte;
- Evaluați activitatea la programe internaționale care vizează domeniul securității cibernetice.

Teme pentru lucrul individual

- Provocări actuale în domeniul securității cibernetice – impact și contribuția Republicii Moldova în domeniu;
- Importanța cooperării în aria securității informaționale/cibernetice;
- Bune practici pentru prevenirea și limitarea efectelor atacurilor cibernetice la nivelul instituțiilor publice din Republica Moldova;
- Mecanisme de cooperare la nivel european/internațional;
- Dezvoltarea cooperării naționale și internaționale.

Bibliografie

1. 14 th International Conference on Cyber Conflict: Keep Moving, CCDCOE Publications. 2022.
https://ccdcoe.org/uploads/2022/06/CyCon_2022_book.pdf 1.
2. ENISA a publicat un raport cu referire la tehnicile de securitate cibernetică pentru protecția datelor
<https://www.enisa.europa.eu/publications/engineering-personal-data-sharing>
3. ENISA a organizat prima conferință de politică în domeniul securității ciberneticice
<https://www.enisa.europa.eu/news/supporting-policy-developments-to-achieve-a-high-common-level-of-cybersecurity>
4. Parteneriatele NATO și Republica Moldova în fața noilor amenințări la adresa securității regionale. Chișinău, 2014, p. 47-49.
5. Cooperare pentru securitate cibernetică. <https://cybersecuritytrends.ro/cooperare-pentru-securitate-cibernetica/>
6. Conferința Internațională cu genericul “Securitatea Cibernetică în Republica Moldova: Provocări, Tendințe și Soluții”. <http://cert.gov.md/news/noutati/article//conferinta.html>
7. Problematika securității ciberneticice în cadrul organizațiilor internaționale și implicarea României ca membru al acestora. <https://www.mae.ro/node/28369>
8. Starea Uniunii 2017 – Securitatea cibernetică: Comisia consolidează răspunsul UE la atacurile ciberneticice. Comisia Europeană - Comunicat de presă. file:///D:/USERS/Corina.Arhiri/Downloads/IP-17-3193_RO.pdf
9. Programul de Securitate Cibernetică. <http://www.mtic.gov.md/ro/projects/programul-de-securitate-cibernetica>
10. Securitatea cibernetică: reguli de protecție împotriva amenințărilor online. <http://www.rfi.ro/politica-88178-securitatea-cibernetica-reguli-de-protectie-impotriva-amenintarilor-online>
11. Мазуров В. Кибертерроризм: понятие, проблемы противодействия. Доклады ТУСУРа, № 1 (21), ч. 1, июнь 2010. с. 41-44
12. Смирнов А. Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза. Москва: ЮНИТИ-ДАНА, 2011.
13. Шрайер Ф., Викс Б., Винклер Т. Кибербезопасность: дорога, которую предстоит пройти. Женева: Женевский Центр демократического контроля над вооруженными силами, 2013. 62 с.
14. Tielidze G., Bagge D., Spinu N. and Ivanović Z. Regional Cyber Security. B: per Concordiam, Vol. 5, issue 2, 2014. p. 24-34
15. Initiative de contracarare a banilor publici, Chisinau, 2015, 86 p.