**USM**

**RELAȚII INTERNAȚIONALE, ȘTIINȚE POLITICE și ADMINISTRATIVE**

**LUCRULINDIVIDUAL**

**TEMA: SECURITATE CIBERNETICĂ**

**( la cursul: Securitatea Informațională)**

**AUTOR TIMUR FLORA**

**GR 02 SNS**

**Chișinău 2023**

**CUPRINS**

1. ÎNTRODUCERE

2.CONCEPTE, DEFINIȚII ȘI TERMENE

3.PRINCIPII

4.VULNERABILITĂȚI, RISCURI ȘI AMENINȚĂRI

5.TIPURI DE ATACURI CIBERNETICE

6.GESTIONAREA RISCURILOR CIBERNETICE

7.MĂSURI DE SECURITĂȚI CIBERNETICE

8.CADRUL LEGISLATIV NAȚIONAL

9.CONCLUZIE

**1.ÎNTRODUCERE**

O definiţia propusă atacului cibernetic este, orice acţiune ostilă desfăşurată în spaţiul cibernetic de natură să afecteze securitatea cibernetică, unde spaţiul cibernetic reprezintă, mediul virtual, generat de infrastructurile cibernetice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori, iar securitatea cibernetică este ,,starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonreproducerea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private din spaţiul cibernetic. Atacul cibernetic urmează aceleaşi etape ca şi celelalte metodologii de atac: obţinerea cât mai multor informaţii despre ţintă, descoperirea punctelor slabe, penetrarea mediului prin exploatarea vulnerabilităţilor identificate în prima etapă, determinarea determinarea şi extinderea posibilităţilor multiple de afectare a ţintei, lansarea atacului propriu zis în vederea obţinerii efectului urmărit, eliminarea oricăror urme care ar putea conduce la identificarea sursei atacului.

Succesul unui atac cibernetic depinde de măiestria cu care atacatorul depistează şi exploatează punctele slabe ale ţintei. Astfel, un sistem cu erori, cu o configuraţie vulnerabilă, cu software antivirus, antifirewall sau de monitorizare a traficului de reţea inexistent sau peste care se poate trece uşor, va deveni cel mai probabil victima unui atac. Căutarea şi identificarea ţintei este prima şi cea mai de durată etapă a unei operaţiuni de acest tip.

Dezvoltarea rapidă a tehnologiilor moderne de informaţii şi comunicaţii - condiţie indispensabilă a edificării societăţii informaţionale - a avut un impact major asupra ansamblului social, marcând adevărate mutaţii atât în filozofia de funcţionare a economicului, politicului şi culturalului, dar şi asupra vieţii de zi cu zi a individului.

Cu cât o societate este mai informatizată, cu atât este mai vulnerabilă, , iar asigurarea securităţii spaţiului cibernetic trebuie să constituie o preocupare majoră a tuturor actorilor implicaţi, mai ales la nivel instituţional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu.

R. Moldova tinde atât la dezvoltarea unui mediu informaţional dinamic bazat pe interoperabilitate şi servicii specifice societăţii informaţionale, cât şi asigurarea respectării drepturilor şi libertăţilor fundamentale ale cetăţenilor şi a intereselor de securitate naţională, întrun cadru legal adecvat.

**2. Concepte, definiţii termeni**

**Ce este securitatea cibernetică?**

Nu există o definiție standard, universal acceptată a securității cibernetice, acest concept acoperă toate garanțiile și măsurile adoptate pentru a apăra sistemele informatice și pe utilizatorii lor împotriva accesului neautorizat, a atacurilor și a prejudiciilor, în scopul de a asigura confidențialitatea, integritatea și disponibilitatea datelor. Securitatea cibernetică implică prevenirea, detectarea incidentelor cibernetice, răspunsul la aceste incidente și redresarea lor ulterioară. Incidentele pot fi provocate intenționat sau nu, pot acoperi diverse situații, ca ex. de la divulgări accidentale de informații până la atacuri asupra întreprinderilor și a infrastructurilor critice, furtul de date cu caracter personal, incidente ce pot avea efecte negative de amploare asupra persoanelor, organizațiilor și comunităților. Conceptul de securitate cibernetică nu se limitează doar la securitatea rețelelor și a informațiilor, ci acoperă orice activitate ilegală care implică utilizarea tehnologiilor digitale în spațiul cibernetic.

**Infrastructuri cibernetice** – infrastructuri de tehnologie a informaţiei şi comunicaţii,constând în sisteme informatice, aplicaţii aferente, reţele şi servicii de comunicaţii electronice.

**Spaţiul cibernetic** – mediul virtual, generat de infrastructurile ciberne, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în spațiul cibernetic.

**Securitate cibernetică** – starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi non-repudierea informaţiilor în forma electronic, a resurselor şi serviciilor publice sau private, din spaţiul cibernetic. Măsurile proactive şi reactive pot include: politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activităţi de instruire şi conştientizare, implementare de soluţii tehnice de protejare a infrastructurilor cibernetice, managementul identităţii, managementul consecinţelor.

**Ameninţare cibernetică** – orice circumstanţă sau eveniment care constituie un pericol potenţialla adresa securităţii cibernetice.

**Atac cibernetic** – orice acţiune ostilă desfăşurată în spaţiul cibernetic de natură să afecteze securitatea cibernetică.

**Incident cibernetic** – orice eveniment survenit în spaţiul cibernetic de natură să afecteze securitatea cibernetică.

**Război cibernetic** – desfăşurarea de acţiuni ofensive în spaţiul cibernetic de către un stat în scopul distrugerii sau perturbării funcţionării infrastructurilor critice ale altui stat, concomitent cu desfăşurarea de acţiuni defensive şi contraofensive pentru protejarea infrastructurii cibernetice proprii.

**Terorism cibernetic** – activităţile premeditate desfăşurate în spaţiul cibernetic de către persoane, grupări sau organizaţii motivate politic, ideologic sau religios ce pot determina distrugeri materiale sau victime de natură să determine panică sau sau teroare.

**Spionaj cibernetic** – acţiuni desfăşurate în spaţiul cibernetic, cu scopul de a obţine neautorizat informaţii confidenţiale în interesul unui stat.

**Criminalitatea informatică** – totalitatea faptelor prevăzute de penală caren reprezintă pericol social şi sunt săvârşite cu vinovăţie, prin intermediul sau asupra asupra infrastructurilor cibernetice.

**Vulnerabilitate** - o slăbiciune în proiectarea şi implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente care poate fi exploatată de către o ameninţare.

**Riscul de securitate** - probabilitatea ca o ameninţare să se materializeze, exploatând o anumită vulnerabilitate specifică infrastructurilor cibernetice.

**Managementul riscului** - un proces complex, continuu şi flexibil de identificare, evaluare şi contracarare a riscurilor la adresa securităţii cibernetice bazată pe utilizarea unor tehnici şi instrumente complexe, pentru prevenirea pierderilor de orice natură.

**Managementul identităţii**  - metode de validare a identităţii persoanelor când acestea accesează anumite infrastructuri cibernetice.

**Rezilienţa infrastructurilor cibernet**ice – capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic şi de a reveni la starea de normalitate

**CERT** – centru de răspuns la incidente de securitate cibernetică –entitate organizaţională specializată care dispune de capabilităţile necesare pentru prevenirea, analiza, identificarea şi reacţia la incidentele cibernetice.

**3. Principii**

La baza realizării securităţii cibernetice stau următoarele ătoarele principii: principii:

-**Coordonarea**-activităţile se realizează într-o concepţie unitară, pe baza unor planuri de acţiune convergente destinate asigurări securităţii cibernetice, în conformitate cu atribuţiile şi responsabilităţile fiec responsabilităţile fiecărei entităţi;

-**Cooperarea**–toate entităţile implicate(din mediul public sau privat) colaborează, la nivel naţional şi internaţional, pentru asigurarea unui răspuns adecvat la ameninţările din spaţiul cibernetic;

**-Eficienţa**–demersurile întreprinse vizează managementul optim al resurselor disponibile;

-**Prioritizarea–**eforturile se vor concentra asupra securizării infrastructurilor cibernetice ce susţin infrastructurile critice naţionale.

-**Diseminarea** – asigurarea transferului de informaţii, expertiză şi bunepractici în scopul protejării infrastructurilor cibernetice.

**4. Vulnerabilități, riscuri și amenințări**

Vulnerabilitatea este o slăbiciune a unui sistem hardware sau software ce permite utilizatorului neautorizat să obțină acces asupra sa. Principalele vulnerabilități în cadrul sistemelor informaționale fiind de natură:

**a)** **fizică** ( ex. atacatorul reușește să pătrundă fizic în incinta sistemelor de calcul și să sustragă informații confidențiale). Pentrua preântâmpina acest lucru trebuie să se asigure secutitatea fizică a echipamentelor de calcul prin plasarea acestora în zone sigure, restricționate personalului neautorizat. Accesul la aceste zone trebuie făcut prin folosirea interfoaneloanelor, cardurilorde acces sau dispozitivelor de scanare a datelor biometrice pentru autentificarea utilizatorilor cu permis de întrare;

O altă vulnerabilitate fizică a sistemelor informatice o reprezintă dezastrele naturale( inundații, cutremure, incendii) sau accidente precum cădere de tensiune sau supratensiune ce pot duce la distrugerera fizică a echipamentelor.

**b) hardware** o atenție deosebită trebuie acordată acestor componente, pentru ca acestea să nu afecteze ulterior buna funcționare a sistemelor informatice. Aceste vulnerabilităîți sunt întâlnite mai des la sistemele de stocarea datelor, fiind cele mai sensibile componente hardware. Din acest punct de vedere se recomandă salvările de siguranță atât la nivelul informațiilor, cât și la nivelul sistemului de operare pentru repunerea rapidăa serviciilor configurate în caz de defecțiune. Se recomandă folosirea metodelor moderne de criptare a datelor, pentru a înlătura aceste vulnerabilități, astfel âncât, în cazul în care datele sunt interceptate ele să nu poată fi decriptate.

**c) software** din acest punct de vedere există mai multe tipuri de vulnedrabilități: ex:cele care mărescprivilegiile utilizatorilor locali fără autorizație; care permit utilizatorilor externi să acceseze sistemul în mod neautorizat; care permit implicarea sistermului într-un atac asupra unui terț utilizator, ex. atacul DdoS (Distributed Denial of Service).

Ameninţările specifice spaţiului cibernetic se caracterizează prin asimetrie şi dinamică accentuată şi caracter global, ceea ce le face dificil de indentificat şi de contracarat prin măsuri proporţionale cu impactul materializării riscurilor.

R. Moldova se poate confrunta zi cu zi cu ameninţări provenite din spaţiul cibernetic la adresa infrastructurilor critice, având în vedere interdependenţa din ce în ce mai ridicată între infrastructurile cibernetice şi infrastructuri precum cele din sectoarele financiarbancar, transport, energie şi apărare naţională. Globalitatea spaţiului cibernetic este de natură să amplifice riscurile la adresa acestora afectând în aceeaşi măsură atât sectorul privat, cât şi cel public. Infrastructurile civile șiu ele au de înfruntat riscuri majore ca și cele de importanțîă publică. Atascuri masive cu viruși informatici ar putea afecta reţelele de control aerian( ex. recent cyber atacul asupra Turkish Airlines din 1 noiembrie 2023 când au fost anulate toate zborurile în ultimul moment între intervalul 19.00-22.00 și în același rând au fost stopate toate vânzările de bilete și chek-in), pe cele ale comerţului internaţional, transferurile de fonduri, precum şi infrastructurile de distribuţie a energiei electrice. Ameninţările la adresa spaţiului cibernetic se pot clasifica în mai multe moduri, dar cele mai frecvent utilizate sunt cele bazate factorii motivaţionali şi impactul asupra societăţii. În acest sens, putem avea în vedere criminalitatea cibernetică, terorismul cibernetic şi războiul cibernetic, având ca sursă atât actori statali, cât şi nonstatali.

Ameninţările din spaţiul cibernetic se materializează - prin exploatarea vulnerabilităţilor de natură umană, tehnică şi procedurală - cel mai adesea în

-atacuri cibernetice împotriva infrastructurilor care susţin funcţii de utilitate publică ori servicii ale societăţii informaţionale a căror întrerupere / afectare ar putea constitui un pericol la adresa securităţii naţionale;

-accesarea neautorizată a infrastructurilor cibernetice;

-modificarea, ştergerea sau deteriorarea neautorizată de date informatice ori restricţionarea ilegală a accesului la aceste date;

-spionajul cibernetic;

-cauzarea unui prejudiciu patrimonial, hărţuirea şi şantajul persoanelor fizice şi juridice, de drept public şi privat.

Pentru diminuarea riscurilor la care sunt expuse sistemele și pentru reducerea potenșialelor pierderi, de regulă sun întroduse diferite tipuri de controale al accesului la sistem. Controalele pot fi preventive, detective sau corective.

Controalele preventive au scop preântâmpoinarea apariției unor incidente în sistem, cele detective vizează descoperirea unor apariții ciudate în sistem, iar controalele corective sunt folosite pentru readucerea la normalitate a sistemului după anumite incidente la care a fost expus.

Ca să poată fi atinse obiectivele enumerate, controalele pot fi administrative, logice tehnice sau fizice.

**Controalele administrative** sunt exercitate prin politici și proceduri, instruire cu scop de conștientizare, verificării generale, verificării de fond înainte de angajare verificării la locurile de muncă, pe timpul concediilor, cursuri de instruire și o supraveghere exigentă.

**Controalele logice sau tehnice** cuprind restricții de accesare a sistemului și măsurile prin care se asigură protecția informațiilor. Din această categorie fac parte sistemele de criptare, carduri inteligente, listele de control al accesului și protocoalele de transmisie.

**Controalele fizice** încorporează, în general,gărzile de protecție și pază, securitatea clădirilor, cum ar fi sistemele de ăncuiere a ușilor, securizarea camerelor cu servere și laptopuri, protecția cablurilor, separarea atribuțiilor de serviciu, realizarea copiilor de siguranțî a fișierilor.

În orice sistem de bariere fizice, sistemul de securitate trebuie să discearnă care sunt persoanele autorizate și care sunt vizitatorii și alte categorii neautorizate. Autentificarea poate fi făcută corpul de pază, alte persoane care se ocupă de controlarea accesului sau sistemele automatr investite cu aceste funcții.

De regulă, identificarea și autentificarea persoanelor se efectuează prin analiza a patru elemente:

**a) ceva ce se află în posesia persoanei,** de regulă fiind chei, cartele magnetice, cartele speciale echipamente de identificare specială, jetoane, ele permițând un prim pas de accesare a sistemului. Există un mare pericol de pierdere a lor sau de dare spre folosință altor persoane;

**b) ceva care individualizează persoana,** identificarea biometrică fiind o variantă de condiționare a accesului. Poate fi amprentele degetelor, buzelor, semnătura, vocea, forma mânii, imaginea retinei, liniile din palmă, imaginea feței. Majoritatea acestor tehnici fiind destiul de scumpe, în comparație cu cele clasice, deseori fiind incomode sau neplăcute la utilizare;

**c) ceva ce persoana știe** de ex. o parolă, însă și ea se află la discreția oamenilor și, de modulde păstrare a secretuluiei sau de ușurința cu care poate fi afiliată, depinde soarta întregului sistem. Sistemul parolelor,cât de complex ar fi el, nu realizează și o securitate totală, depinzând în mod substanțial de modul de păstrare a secretului parolei. Regulile impuse de controlare a parolelor sunt:

- trebuie să fie schimbate odată la șase luni, dar pentru datele deosebit de importante se impun termene și mai scurte;

- parolele comune trebuie schimbate imediat ce o persoană părăsește grupulsau nu mai are dreptul utilizării lor;

- parolele trebuie schimbate imediat ce se constată unele bănueli privind cunoașterea lor de persoane neautorizate;

- parolele trebuie să fie ținute minte și nu scrise oriunde, excepție fiind cazurile: trebuie să fie scrise pentriu intervenție de urgrnță; fiecare parolă scrisă să fie întrodusă într-un plic sigilat și marcat în exterior cu scurte detalii privind calculatorul la care poate fi folosită și numele celor autorizați de a le folosi; după ruperea sigiliului, pe plic vor fi scrise data și numele celor ce au aflat-o; plicurile cu parole se păstrează de către responsabilul cu securitatea sistemului;

- paroleele nu vor fi afișate niciodată pe echipamentele din configurația sistemului, iar la întroducerea lor de la tastatură nu trebuie să se sfle persoane străine în preajmă;

- parolele, în cele mai multe cazuri au cel puțin 8 caractere, ele fiind caractere alfanumerice- litere mari și mici, cifre și spații, folosite ăn ordine aleatoare, ceea ce ar însemna câteva mii de cuvinte de opt sau mai puține caractere, care pot fi testate cu ajutorul calculatorului, în doar câteva minute, deci sunt destul de vulnerabile pentru „profesioniștii„ de spargrre de sisteme;

- pentru blocarea operațiunilor de încercare repetetă, de ordinul miilor, calculatoarele trebuie să permită in număr limitat de încercări de întroducere a acestora, uzual de trei ori. Dacă limita a fost depășită,de către utilizator, intenția trebuie să fie raportată conducătorului sistemului sau responsabilului de securitate.

**d) locul geografic unde este înregistrat calculatorul.**

Metodele de controlare a accesului trebuie să se bazaze pe cel puțin două dintre cele patru enumerate: deseori se apelează la combinațiile cartelă-parolă, cheie-parolă, jeton-parolă. În ultimul timp se recomandă ca în sistemele de protecție să se folosească tot mai mult elwmentul biometric.

**Principalii actori care generează ameninţări în spaţiul cibernetic:**

-persoane sau grupări de criminalitate organizată care exploatează vulnerabilităţile spaţiului cibernetic în scopul obţinerii de avantaje patrimoniale sau nepatrimoniale;

-terorişti sau extremişti care utilizează spaţiul cibernetic pentru desfăşurarea şi coordonarea unor atacuri teroriste, activităţi de comunicare, propagandă, recrutare şi instruire, colectare de fonduri, în scopuri teroriste. Grupările teroriste pot plăti hakeri pentru aşi realiza scopurile şi a lansa atacuri asupra reţelelor infrastructurale;

-state sau actori nonstatali care iniţiază sau derulează operaţiuni în spaţiul cibernetic în scopul culegerii de informaţii din domeniile guvernamental, militar, economic sau al materializării altor ameninţări la adresa securităţii naţionale.

**CINE SUNT HACKERII?** Organizațiile se confruntă cu amenințări la adresa informațiilor și a securității cibernetice de la o gamă largă de actori. Hackerii "cu pălării negre" (“black hat” hackers) și infractorii cibernetici au încercat să compromită campanii din diverse motive: câștig personal, notorietate sau simpla dorință de a-și pune la încercare abilitățile. Un hacker este un expert, care se ocupă cu studii în profunzime alprogramelor informatice( sisteme de operare, aplicații), adesea folosind tehnici de inginerie inversă (demontare), cu scopul de a obține cunoștințe care nu sunt accesibile publicului larg). Cei ce folosesc aceste cunoștințe în scopurile ilegale, pentru a compromite securitatea sistemelor informatice sau a aplicațiilor sunt de fapt **crackeri** (spărgători), în percepția publicului larg noțiunile de hacker și crackeri adesea se confundă.Țările străine reprezintă cea mai dedicată și persistentă amenințare. Grupurile de spionaj rusesc cunoscute sub numele de "Fancy Bear" (APT 28) și "Cozy Bear" (APT 29) au fost implicate în hack-urile de campanie din 2016 din SUA. Chinezii s-au concentrat mult mai mult pe colectarea informațiilor. Se crede că aceștia au fost activi în campaniile prezidențiale din 2008 și 2012 ale SUA, dar nu există dovezi că au scurs informații. Nord-coreenii s-au răzbunat pe compania Sony Pictures Entertainment pentru producția filmului “The Interview”: au furat și scurs emailurile companiei și au șters sistemele lor. În unele țări, campaniile opoziției sunt amenințate și de propriul guvern.

**5.Tipuri de atacuri cibernetice**

**1) Programele malware (** sowtware rău-intenționat) sunt concepute cu scopul de a perturba funcționarea dispozitivelor sau a rețelelor. Acestea includ **viruși, trocini, ransomware, viermi informatici, adware și spyware.** Programele *ransomware* criptează datele, împiedicând utilizatorii să aibă acces la fișierile lor pânî când nu este plătită o răscumpărare, de regulă criptomonedă, sau până când se efectuează o anumită acțiune. Aceste atacuri sunt predominante, numărul lor crescând esențial. De asemenea sunt în creștere atacurile de tip *DDoS,*care blochează anumite servicii sau resurse prin atacul lor cu mai multe cereri decât pot fi prelucrate.

Spionajul cibernetic sau furtul de date cunoscut sub denumirea de „*inginerie socială„*, prin acest mijloc utilizatorii pot fi manipulați să efectueze în mod neintenționat o anumită acțiunesau să divulge informații confidențiale. Există mai multe mijloace utilizate în acest scop, o metodărăspândită fiind cea a *phishingului:* prin e-mailuri care par a fi provenite din surse de încredere, utilizatorii sunt duși în eroare să dezvăluie informații sau să deschidă lincuri care vor infecta dispozitivele cu programe malware descărcate.

Un alt tip de atac cibernetic sunt așa-numitele „*amenințări persistente avansate„ ( ART-advansed persistent threats),* fiind vorba de acțiuni sofisticate,în care atacatorii sunt angajați pe termen lung de monitorizare și de furt de date, uneori avân scop și de distrugere. Obiectivul urmărit este ca atacatorii să rămână cât mai multposibil nedescoperiți.

**6.Gestionarea riscurilor cibernetice**

Riscul este cel mai bine perceput prin trei componente. În primul rând, există vulnerabilități: slăbiciunile campaniei,instituției organizației, care fac informațiile susceptibile la furt, modificare sau distrugere. Vulnerabilitățile pot apărea în hardware, software, procese și în nivelul de vigilență al personalului.

Apoi, există amenințări reale: țări străine, hackeri și alte grupuri cu capacitatea de a exploata aceste vulnerabilități. Riscul apare atunci când există vulnerabilități și amenințări.

În cele din urmă, există consecințe—impactul produs de actorii cu rea intenție care profită de riscuri, nu se poate face multe pentru a preveni amenințările în sine—ele sunt rezultatul unor forțe geopolitice, economice și sociale mai mari. Ceea ce putem face, însă, este să reducem substanțial posibilitatea succesului adversarilor , eliminând propriile vulnerabilități. Reducerea vulnerabilității reduce riscul—decidem pe care le reducem în mod prioritar. Bunăoară, am putea decide că cel mai dăunator lucru pe care vi-l poate fura un hacker este raportul de autoanaliză a candidatului (ex. în campanie electorală), așa că vom aloca resurse suplimentare pentru o stocare sigură online, care impune utilizarea parolelor lungi și restricționează accesul la un număr mic de persoane. Există aspecte tehnice de atenuare a riscurilor, însă cel mai mult contează abordarea noastră holistică. În calitate de lider al unei instituții, organizații, cel mai important lucru pe care îl putețem face este luarea deciziilor fundamentale: cine are acces la informații, care informații sunt păstrate sau șterse, cât timp dedicăm pentru instruiri, dar și propriul nostru comportament în instituții/organizații.

Securizarea instituțiilor/organizațiilor trebuie să fie organizate organizate după trei principii:

**-1. Pregătiți-vă:** Succesul major depinde de crearea, de către conducere a unei culturi de vigilență în domeniul securității, care minimizează punctele slabe. Aceasta înseamnă stabilirea unor reguli clare, care să fie impuse de sus în jos și respectate de jos în sus.

-**2. Protejați-vă**: Protecția este crucială. De obicei, atunci când descoperim că avețm o problemă de securitate, este deja prea târziu. Construcția celei mai puternice protecții pe care putem să ne-o permitem cu timpul și banii disponibili, este esențială pentru reducerea riscului. Securitatea online și protecția datelor funcționează cel mai bine în straturi: nu există o singură tehnologie sau produs universal de protecție. Combinând câteva măsuri de bază, putem face arhitectura digitală a instituției/organizației, mai greu de pătruns și mai rezistentă, în cazul în care este compromisă, economisind astfel timp și bani pe care le-am putea pierde în viitor

**-3. Persistați**: Acum, adversarii au tot mai multe resurse și expertiză; chiar și cea mai vigilentă cultură și cea mai dură infrastructură ar putea să nu fie capabile să împiedice o breșă de securitate. I nstituțuiile/organizațiile trebuie să elaboreze din timp un plan pentru a face față unei eventuale breșe.

**7.Masuri de securități cibernetice**

Una dintre cele mai ieftine si mai simple miscari pe care le pot face companiile mici in domeniul securitații cibernetice este utilizarea unor parole puternice. Folosirea unor parole puternice este echivalent cu un grad de complexitate ridicat al acestora, dificil de ghicit de hackeri, crachkeri si care sa aiba cel putin opt caractere. Astfel, o de genul "tnt@mZ1y2qXOG" este mult mai bună decât "superman".

**1. stabilirea cadrului conceptual, organizatoric şi acţiunile necesare asigurării securităţii cibernetice.**

a)constituirea şi operaţionalizarea unui sistem naţional de securitate cibernetică;

b)completarea şi armonizarea cadrului legislativ naţional în domeniu, inclusiv stabilirea şi aplicarea unor cerinţe minime de securitate pentru iinfrastructurile cibernetice naţionale;

c)dezvoltarea unui parteneriat public-privat, inclusiv prin stimularea schimbului reciproc de informaţii, privind ameninţări, vulnerabilităţi, riscuri, precum şi incidente de atacuri cibernetice.

**2. dezvoltarea capacităţilor naţionale de management al riscului în domeniul securităţii cibernetice şi de reacţie la incidente incidente cibernetice în baza unui program naţional** ce ar viza

a)Consolidarea, la nivelul autorităţilor competente competente potrivit legislației, a potenţialului de cunoaştere, prevenire şi contracarare a riscurilor asociate utilizării spaţiului cibernetic;

b) asigurarea unor instrumente de dezvoltare a cu toate sectoareleîn domeniul securităţii cibernetice, inclusiv pentru crearea unui mecanism eficient de avertizare şi alertă, de reacţie la incidentele cibernetice;

c) stimularea capabilităţilor naţionale de cercetare-dezvoltare şi inovare în domeniul securităţii cibernetice;

d) creşterea nivelului de rezilienţă a infrastructurilor cibernetice. Dezvoltarea entităţilor de tip CERT.

**3. Promovarea şi consolidarea culturii consolidarea culturii de securitate în domeniul cibernetic**

a)derularea unor programe de conştientizare a populaţiei, a administraţiei publice şi a sectorului cu privire la vulnerabilităţile, riscurile şi ameninţările specifice utilizării spaţiului cibernetic;

b)formarea profesională adecvată a persoanelor care îşi desfăşoară activitatea în domeniul securităţii cibernetice şi promovarea pe scară largă a certificatelor profesionale în domeniu.

c) includerea unor elemente referitoare la securitat securitatea cibernetică în programele de formare şi perfecţionare profesională a managerilor din domeniul public şi privat.

**4. Dezvoltarea cooperării internaţionale în domeniul securităţii cibernetice**

a) încheierea de acorduri de cooperare la nivel internaţional pentru îmbunătăţirea capacităţii de răspuns în cazul unor atacuri cibernetice majore;

b) participarea la programe internaţionale care vizează domeniul securităţii cibernetice;

c) promovarea intereselor naţionale de securitate cibernetică în formatele de cooperare internaţională la care Moldova este parte.

**8.Cadrul legislativ național**

**-**Constituția R.M ( ex Titlul II, cap.2);

- Legea Nr 467 din 21-11-2003 cu privire la informatizare și la resursele informaționale de stat;

- Hotărârea Nr.257 din 22-11-2018 privind aprobarea Strategiei securității informaționale a R.M. pentru anii 2019-2024 și a Planului de acțiuni pentru implimentarea acesteia;

- Legea Nr.133 din 08-07-2011 privind protecția datelor cu caracter personal;

Legea Nr 142 din 19-07-2018 cu privire la schimbul de date și interoperabile;

-Legea Nr.124 din 19-05-2022 privind identificarea electronică și servici de încredere;

- Hotărârea Nr HG201/2017 din 2018 privind aprobarea cerințelor minime obligatorii de securitate ciberbetică.

- Legea privind securitatea cibernetică adoptată la 10.03.2023, care va intra în vigoare de la tata de 01.01.2025; ș.a..legi privind drepturile și interesele ce țin de căutarea, primirea,transmiterea, răspândirea, formarea, prelucrarea, păstrarea, utilizarea și protecția informației.

**9.Concluzie**

Dinamica mediului informațional dată de schimbările tehnologice rapide și continue cât și apariția de noi cerinâe din partea organizațiilor/insiituțiilor supune și sistemul informatic la noi dezvoltări, asigurarea unei activități corespunzătoare de procesare implică și oplanificare riguroasă a activităților sprijinite de sistemul informațional. În ultimii ani spațiul cibernetic devine din ce în ce mai militarizat și este transformat pe zi ce trece într-o armă, ajuns să fie considerat al cincele câmp de luptă. Apărarea cibernetică protejează sistemele, rețelele și infrastructurile criticedin spațiul cibernetic împotriva atacurilor militare și de orice alt tip. UE a actualizat cadreu de politici pentru apărarer cibernetică, care identifică șase priorități, cum ar fi: dezvoltarea capacităților de apărare cibernetică și protejarea rețelilor de comunicații și de informații din cadrul politicii de securitate și apărare comună PSAC a UE, apărarea cibernetică mai făcând parte și din cadrul de cooperare structurată permanent PESCO și din cooperarea UE-NATO.

**Bibliografie**

1. David A, Pașca V, Tanase T, Războiul informațional-delimitări conceptuale, forme de manifestare, medii și valori vizate, modalități de contracarare, București, 2005;

2. Codreanu I, Opriș M, Cyberterorizmul-o nouă amenințare la adresa securității naționale, București 2007;

3.Gifu I, Nantoi O, Războiul informațional. Tipizarea modelului agresiunii, Editura Institutului de științe politice și Relații Internaționale „Ion I.C.Brătianu”al Academiei Române, București 2016;

4. Concepția securității informaționale a R. Moldova;

5.Ghid de securitate cibernetică pentru funcționarii publici, Serviciul Tehnologia Informației și Securitatea cibernetică 2018:

6. Ghid de bune practici pentru securitatea cibernetică, Serviciul Român de Informație, [www.sri.ro](http://www.sri.ro);

7. Legea Nr 467 din 21-11-2003 cu privire la informatizare și la resursele informaționale de stat;

8.Legea privind securitatea cibernetică adoptată la 10.03.2023, care va intra în vigoare de la tata de 01.01.2025

9. Hotărârea Nr HG201/2017 din 2018 privind aprobarea cerințelor minime obligatorii de securitate ciberbetică.