Curs 1

1) Sistem numeric de comunicaţie. Schema bloc şi explicaţie.

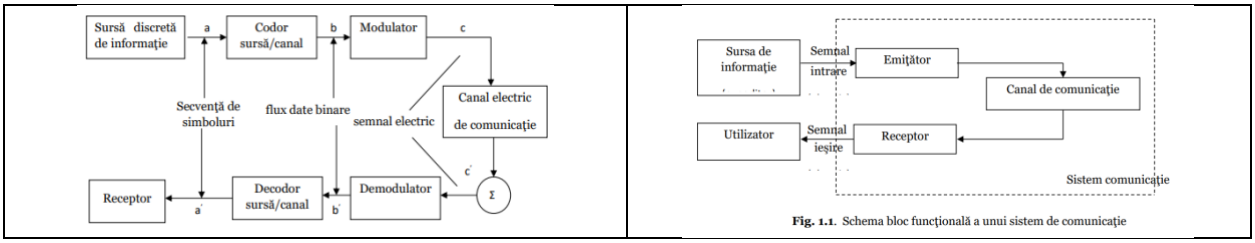


Fig. 1.1. Schema bloc funcţională a unui sistem de comunicaţie

a) sursa de informaţie

Există 2 categorii, după natura semnalului de ieşire: surse analogice (continue) & surse numerice (discrete).

b) blocuri de codare/decodare

Intrarea în codor este o secvenţă de simboluri ce apar cu viteza vs (simb/s). Codorul sursă converteşte secvenţa de simboluri într-o secvenţă de valori binare 0 sau 1, iar codorul canal grupează aceste simboluri binare în cuvinte. surse numerice (discrete).

c) blocuri modulator/demodulator

Modulatorul asigură minimizarea efectelor perturbatoare ale canalului, prin folosirea unor semnale de putere şi bandă sporită. Demodulatorul are drept efect extragerea mesajul din semnalul obţinut la ieşirea canalului, prin tehnici adecvate ce depind evident de tipul de modulaţie utilizat.

d) canal de comunicaţie

Este un circuit fizic de tip electric/electromagnetic, cu o bandă de trecere limitată şi un anumit efect atenuator asupra semnalului.

2) Informaţie. Unitatea de măsură a informaţiei. Relaţie de calcul şi definiţie.

Informaţia care se obţine prin realizarea evenimentului xi de probabilitate pi va fi:

$I(x_i) = -k \log_b p(x_i)$, cu $k = k(b)$, unde b este unitatea

Se defineşte bit-ul ca informaţia care se obţine prin realizarea unui eveniment din două evenimente echiprobabile.

$$I = -\log_2 \frac{1}{2} = 1bit$$

Bit-ul este unitatea de măsură a informaţiei.

Curs 2+3

1. Definiţi proprietăţile de staţionaritate şi regularitate ale unei surse de informaţie.

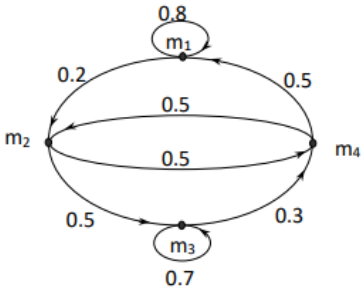
   Proprietățile unei surse de informație sunt următoarele:
   a) Staționaritate: O sursă de informație este considerată staționară dacă distribuția probabilităților pentru simbolurile sau evenimentele sale nu se schimbă în timp. Aceasta înseamnă că probabilitățile de apariție a simbolurilor rămân constante indiferent de momentul în care sunt observate. Un sistem staționar produce informații cu caracteristici constante în timp.

   b) Regularitate: O sursă de informație este considerată regulată dacă simbolurile sau evenimentele pe care le generează sunt independente între ele. Cu alte cuvinte, apariția unui simbol nu depinde de simbolurile anterioare sau ulterioare din cadrul sursei. O sursă regulată nu are nicio structură sau model intern, iar fiecare simbol este generat independent de celelalte.

2. Ce este o sursă fără memorie? Dar o sursă cu memorie? Prezentaţi caracteristicile acestora

Sursă fără memorie (sursă Markov de ordinul 0)	**Sursă cu memorie**
o sursă de informație care generează simboluri sau evenimente independente între ele. Apariția fiecărui simbol nu depinde de istoricul sau contextul din sursele anterioare. Cu alte cuvinte, fiecare simbol este generat independent de ceilalți și nu se bazează pe informații anterioare.	o sursă de informație în care apariția simbolurilor este influențată de simbolurile anterioare. Simbolurile generate sunt dependente de contextul și istoricul din sursele anterioare.
Caracteristici: • Absența dependenței de istoric: Probabilitatea apariției unui simbol este fixă și nu este influențată de simbolurile anterioare. • Distribuție constantă: Probabilitățile de apariție a fiecărui simbol rămân constante în timp. • Lipsa structurii interne: Nu există o legătură sau o dependență între simbolurile generate.	Caracteristici: • Dependența de istoric: Probabilitatea apariției unui simbol depinde de simbolurile anterioare și poate fi influențată de acestea. • Distribuție variabilă: Probabilitățile de apariție a simbolurilor pot varia în funcție de contextul și istoricul din sursele anterioare. • Există o structură internă: Simbolurile generate au o legătură sau o dependență între ele, determinată de contextul și istoricul din sursele anterioare.

3. Explicarea unei surse de tip Markov cu 4 stări + construirea matricei probabilitatilor de tranzitie



$$\Phi = \begin{bmatrix} 0.8 & 0.2 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.5 & 0.5 \\ 0.0 & 0.0 & 0.7 & 0.3 \\ 0.5 & 0.5 & 0.0 & 0.0 \end{bmatrix}$$

Fig. 2.1. Sursă Markov cu patru stări - graf şi matrice probabilităţi de tranzitie

Sursele Markov discrete pot fi reprezentate prin grafuri orientate cu arce de "capacităţi" egale cu probabilităţile tranziţiilor asociate. Aceste probabilităţi, ca şi graful însuşi, se pot reprezenta şi sub formă matricială, cu respectarea condiţiei ca suma probabilităţilor pe fiecare linie a matricii să fie egală cu unitatea.

Considerând o sursă de informaţie având ca model un proces Markov aleator, ergodic şi discret, cu graful asociat prezentat în figura 2.1, se poate calcula entropia sursei şi informaţia medie pe simbol conţinută în mesaje de 1, 2 şi 3 simboluri.

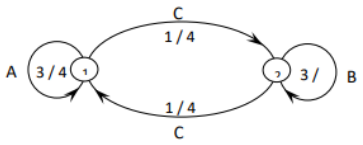


Fig. 2.2. Graful asociat sursei de informaţie

În tabelul 1.1 sunt ilustrate probabilităţile de apariţie ale tuturor mesajelor de lungimi de 1 simbol, 2 simboluri şi 3 simboluri.

Tabel 1.1. Probabilităţi apariţie mesaje

Mesaje de lungime 1	Mesaje de lungime 2	Mesaje de lungime 3
A (3/8)	AA (9/32)	AAA (27/128)
B (3/8)	AC (3/32)	AAC (9/128)
C (1/4)	CC (2/32)	ACC (3/128)
	CB (3/32)	ACB (9/128)
	CA (3/32)	CCA (3/128)
	BC (3/32)	CCC (2/128)
	BB (9/32)	CBC (3/128)
		CBB (9/128)
		CAA (9/128)
		CAC (3/128)
		CCB (3/128)
		BCA (9/128)
		BCC (3/128)
		BBC (9/128)
		BBB (27/128)

Se calculează: H1 = H2 =1/4 log 1/4 +3/4 log 3/4 = 0,8113 bit / simbol; H = 1/2 H1 + 1/2 H2 = 0,8113 bit / simbol. Calculând informaţia medie conţinută în mesajele de două simboluri, se obţine: I (AA) = I (BB) = 1,83; I (BC) = I (AC) = I (CB) = I (CA) = 3,415 biţi.

4. Entropia informationala, definitii, relatii de calcul, proprietati (maxim 3)

Măsura nedeterminării unui experiment cu n evenimente a1,...,an, caracterizate de probalitati $p_1,\ldots,p_n, p_i \geq 0, \sum_1^n p_i = 1$, este expresia $H(p_1, p_2,\ldots,p_n) = -\sum_1^n p_i \log p_i$ şi este denumită entropie.

Proprietăţile ale entropiei:

1.Cu conditia p log p =0, daca p=0, entropia este o functie pozitiva, simetrica si continua.

2. $(\forall) p_1, p_2,\ldots,p_N, H(p_1, p_2,\ldots,p_n) \leq H\left(\frac{1}{n}, \frac{1}{n},\ldots,\frac{1}{n}\right)$

Entropia este maxima atunci cand prob p1...pn sunt egale.

3.Prin impartirea unui eveniment in cat mai multe evenimente, entropia nu scade, ci creste.

Curs 4+5

1. Caracteristica entropica a unui sistem de transmisii de date

Sursa este definită de un număr de stări, uzual finit, şi generează un număr de simboluri x1, x2,..., xn cu probabilităţile p(x1), p(x2),...,
p(xn), având suma egală cu unitatea. Rezultă că sursa este caracterizată de entropia

$$H(X) = -\sum_1^n p(x_i) \log p(x_i)$$

Receptorul este, de asemenea, definit de un număr de stări asociate cu simbolurile x1, x2,..., xm şi cu probabilităţile p(x1), p(x2),..., p(xm). Recepţia este caracterizată de entropia

$$\mathrm{H(X)} = -\sum_{\mathrm{j=1}}^{\mathrm{m}} \mathrm{p(x_j) \log p(y_j)}$$

Echivocaţia H(x/y) este definită ca fiind măsura echivocului care există asupra câmpului de intrare *X* când se cunoaşte câmpul de ieşire Y.
Eroarea medie H(x/y) de transmisie este definită ca măsura incertitudinii care există asupra câmpului de ieşire când se cunoaşte câmpul de intrare.

2. Formula HTS (enunț + relație de calcul)

Formula Hartley-Tuller-Shannon defineşte capacitatea temporală, Cτ sau debitul de transmitere a informaţiei pe canal

$$C_\tau = D_t = B\log\left(1+\frac{s}{z}\right)\ [bit/s],$$

,unde B defineşte banda de trecere, iar s, z puterile semnalului, respectiv ale zgomotului, cu s/z - raportul semnal-zgomot.

Formula Hartley-Tuller-Shannon are aplicaţii practice, fiind foarte utilă pentru că subliniază corelaţia între banda de trecere şi raportul semnal–zgomot (unul dintre aceşti doi factori creşte în detrimentul celuilalt).

De asemenea, formula Hartley-Tuller-Shannon arată că pe un canal având C < v (capacitatea canalului mai mică decât viteza sursei) nu este posibilă transmisia fără eroare.

Invers, impunând o anumită viteză de transmisie şi cunoscând B, se poate calcula raportul s / z minim. Mai mult, capacitatea canalului nu poate creşte oricât, numai prin creşterea benzii B, dacă raportul s/z rămâne acelaşi. Capacitatea temporală a unui canal are o limită.

Curs 6+7 (nu a dat la partial si nu da nici la examen)

Curs 8+9

1. **Cod, codificare, cuvant de cod, definitii si decodificare**

Fie o sursă discretă, fără memorie, având alfabetul $S = \{S_1, S_2, \ldots, S_N\}$ cu probabilităţile de apariţie asociate $p(S_i) = p_i$

Orice aplicaţie $S \to X^*$ se numeşte ***codificarea*** ansamblului S prin alfabetul X.

Elementul lui X^*, S_i^* ce corespunde lui S_i, este un ***cuvânt de cod.*** Totalitatea cuvintelor de cod constituie ***codul*** lui S Totalitatea cuvintelor de cod constituie ***codul*** lui X^* poate conţine şi combinaţii care nu aparţin codului,

numite *cuvinte fără sens.Un cod este o corespondenţă biunivocă între mulţimea mesajelor sursă şi o mulţime de cuvinte de cod.*
***Decodificarea** presupune transformarea unei codificări într-un număr real, folosind probabilități de apariție a simbolurilor și numărul total de simboluri codificate. Se utilizeaza un algoritm de decompresie si se începe cu un interval inițial [a; a + l), unde a = 0 și l = 1 și se caută subintervalul corespunzător numărului de decodificat. Se transmit simbolurile corespunzătoare și intervalul se actualizează. Procesul se repetă până la decodificarea tuturor simbolurilor sau până la identificarea simbolului de sfârșit al codificării.*

2. Sursa, Sistemul de transmisie, metode de codificare: Shannon-Fano, Huffman-Schwartz, Codificare aritmetica

O **sursă** reprezintă originea informației într-un sistem de comunicații și poate fi o sursă de date, de semnale sau de informație.

Un **sistem de transmisie** este un ansamblu de componente și tehnologii utilizate pentru a transfera semnale sau date de la o sursă la un destinatar prin intermediul unui mediu de transmisie (cum ar fi cabluri, unde radio sau fibră optică).

Metoda de codificare Shannon-Fano este o tehnică de codificare a datelor în care fiecărui simbol sau eveniment îi este atribuit un cod unic. Codurile sunt atribuite în funcție de probabilitățile de apariție a simbolurilor, iar simbolurile cu probabilități mai mari primesc coduri mai scurte. Această metodă se bazează pe principiul deciziei în care se încearcă să se minimizeze numărul mediu de biți necesari pentru a reprezenta un simbol.

Shannon-Fano:
1)Se calculează probabilitățile de apariție pentru fiecare simbol.
2)Se sortează simbolurile în funcție de probabilități, în ordine descrescătoare.
3)Se împarte lista de simboluri în două părți aproximativ egale, astfel încât suma probabilităților din fiecare parte să fie cât mai aproape de jumătatea totală a probabilităților.
4)Se atribuie codul "0" pentru simbolurile din prima parte și codul "1" pentru cele din a doua parte.
5)Procesul se repetă recursiv pentru fiecare parte până când fiecare simbol primește un cod unic.

Exemplu Shannon-Fano:
Simboluri: A, B, C, D
Probabilități: 0.4, 0.3, 0.2, 0.1

Pasul 1: Sortare
Simboluri: A, B, C, D
Probabilități: 0.4, 0.3, 0.2, 0.1

Pasul 2: Împărțire
Simboluri: A, B | C, D
Probabilități: 0.4, 0.3 | 0.2, 0.1

Pasul 3: Atribuire coduri
Simboluri: A, B | C, D
Coduri: 0, 1 | 00, 01

Pasul 4: Recursivitate
Simboluri: A | B
Coduri: 0 | 1

Metoda de codificare Huffman-Schwartz este o tehnică de compresie a datelor care utilizează un arbore Huffman pentru a atribui coduri cu lungimi variabile fiecărui simbol. Simbolurile cu probabilități mai mari de apariție primesc coduri mai scurte, ceea ce duce la o compresie eficientă a datelor. Această metodă se bazează pe algoritmul Huffman, care construiește un arbore optimal pe baza probabilităților de apariție a simbolurilor.

Huffman-Schwartz:
1)Se calculează probabilitățile de apariție pentru fiecare simbol.
2)Se construiește un arbore Huffman, unde simbolurile sunt frunze și se utilizează un algoritm de construcție a arborelui bazat pe probabilități.
3)Codurile sunt atribuite pe baza poziției în arbore, astfel încât să se obțină coduri mai scurte pentru simbolurile cu probabilități mai mari și coduri mai lungi pentru cele cu probabilități mai mici.

Exemplu HS

Exemplificarea foloseşte acelaşi şir de opt mesaje codificate anterior.

0,35	0,35	0,35	0,35	0,35	0,4	0,6 | 0
0,23	0,23	0,23	0,23	0,25	0,35 | 0	0,4 | 1
0,14	0,14	0,14	0,17	0,23 | 0	0,25 | 1	
0,1	0,1	0,11	0,14 | 0	0,17 | 1		
0,06	0,07	0,1 | 0	0,11 | 1			
0,05	0,06 | 0	0,07 | 1				
0,04 | 0	0,05 | 1					
0,03 | 1						

Codurile obţinute pentru mesaje sunt următoarele:
0,35 – cod 00
0,23 – cod 10
0,14 – cod 010
0,10 – cod 110
0,06 – cod 0110
0,05 – cod 0111
0,04 – cod 1110
0,03 – cod 1111

Codificarea aritmetică este o tehnică de compresie a datelor care atribuie un singur număr real între 0 şi 1 pentru a reprezenta întreaga secvenţă de simboluri. Intervalul este împărţit în subintervale corespunzătoare probabilităţilor de apariţie a simbolurilor, iar secvenţa de simboluri este reprezentată de numărul real care se află în subintervalul corespunzător. Această metodă oferă o compresie foarte eficientă, dar necesită operaţii aritmetice precise pentru a decoda informaţiile.

Codificarea Aritmetică:

1)Se calculează probabilităţile de apariţie pentru fiecare simbol.
2)Se construieşte un interval iniţial [a, b) care acoperă întregul interval [0, 1).
3)Intervalul este împărţit în subintervale corespunzătoare probabilităţilor de apariţie a simbolurilor.
4)Fiecare simbol este reprezentat prin valoarea reală din subintervalul corespunzător.
5)Procesul se repetă pentru fiecare simbol în succesiune, actualizând intervalul în funcţie de subintervalele corespunzătoare.

Exemplu:
Simboluri: A, B, C, D
Probabilităţi: 0.4, 0.3, 0.2, 0.1

Pasul 1: Interval iniţial [a, b)
[a, b) = [0, 1)

Pasul 2: Împărţirea intervalului
[a, b) = [0, 0.4) pentru A
[a, b) = [0.4, 0.7) pentru B
[a, b) = [0.7, 0.9) pentru C
[a, b) = [0.9, 1) pentru D

Pasul 3: Reprezentare simboluri
Simboluri: A, B, C, D
Reprezentare: 0.2, 0.55, 0.8, 0.95

Repetarea paşilor 2 şi 3 pentru fiecare simbol în succesiune.

Curs 10+11

1. Definiţi distanţa Hamming. Proprietăţi.

   Distanţa dintre două cuvinte binare de lungime n, de forma $u = x_1,\ldots,x_n$, $v = y_1,\ldots,y_n$, este dată de numărul poziţiilor de acelaşi rang în care acestea diferă $d(u,v) = \sum_{i=1}^{n} x_i \oplus y_i$. Proprietăţile distanţei Hamming sunt cele ale unei distanţe, anume
   $d(u,v) = d(v,u) \geq 0$, $d(u,v) = 0 \Leftrightarrow u = v$ si $d(u,v) \leq d(u,w) + d(w,v)$.

2. Prezentaţi semnificaţia teoremei fundamentale a transmisiei informaţiei in contextul canalelor perturbate .
   Teorema fundamentală a teoriei informaţiei se referă la posibilitatea ca o sursă de entropie $H < C$, cu C - capacitatea sursei, să fie codată astfel încât rata de emisie R să fie oricât de apropiată de C.
   Concluzia teoremei este aceea că pentru a micşora eroarea trebuie să fie crescută lungimea cuvântului de cod. Pe de altă parte, în practică trebuie să se utilizeze cuvinte de cod cât mai scurte. Este deci necesar să se ajungă la un compromis între eliminarea perturbaţiilor şi creşterea eficienţei. Acest lucru este realizabil fie prin creşterea debitelor, fie prin utilizarea unor algoritmi rapizi de decodificare.

3. Ce este un cod Hamming? Cum sunt clasificate aceste coduri?

   Codurile Hamming sunt coduri de grup pentru care biţii de control sunt determinaţi în funcţie de biţii informaţionali prin relaţii de condiţie care asigură paritate prin suma modulo 2. Codurile Hamming pot fi: - sistematice, caz în care primii m biţi sunt informaţionali; - ponderate, atunci când biţii de control apar pe poziţii corespunzătoare puterilor lui 2 (poziţiile 1, 2, 4, 8, …).

   Cuvintele de cod Hamming sunt formate dintr-un număr total de n biţi; biţii purtători de informaţie sunt în număr de m şi formează partea semnificativă a cuvântului de cod, iar n-m=k biţi sunt biţi de control care formează partea de test a cuvântului de cod.

4. Definiţi codurile ciclice. Prezentaţi sintetic metodele de construcţie asociate.

Un cod liniar este ciclic dacă orice permutare ciclică a unui cuvânt de cod este, de asemenea, un cuvânt de cod. Astfel, dacă se consideră cuvântul de cod $u = a_1a_2a_3…a_{n-1}a_n$, prin deplasarea în inel a simbolurilor care alcătuiesc cuvântul de cod se obţine tot un cuvânt de cod.

Metodele de construcţie a codurilor ciclice folosesc două modalităţi de exprimare a polinomului de cod u(x):

- cu evidenţierea părţii semnificative (informaţionale) s(x) şi a părţii de test t(x), sub forma u(x)=s(x)+t(x) ;
- cu evidenţierea proprietăţii oricărui cuvânt de cod ciclic de a se divide cu un polinom generator g(x), sub forma u(x)=g(x)q(x).

Pentru generarea codurilor ciclice sunt utilizate următoarele patru metode: metoda directă; metoda matricii generatoare; metoda matricii de control; metoda rădăcinilor polinomului generator.

Curs 12

1. Definiţi conceptul de virus informatic. Surse de provenienţa.
   Virusul informatic este o formă de software malicios care are capacitatea de a se reproduce și răspândi în sistemul informatic al unui utilizator fără consimțământul acestuia. Virusul poate infecta fișiere, programe sau chiar întregul sistem, provocând daune și perturbând funcționalitatea normală a computerului. Există mai multe surse de proveniență pentru viruși informatici, inclusiv:
   - Descărcarea de pe internet: Virușii pot fi distribuiți prin intermediul fișierelor descărcate de pe internet, cum ar fi programe, jocuri sau conținut media. Aceste fișiere pot conține coduri malitioase care sunt activate odată ce sunt descărcate și executate.

   - E-mail-uri și atașamente: Virușii pot fi transmiși prin intermediul mesajelor de e-mail și a fișierelor atașate. Utilizatorii pot fi înșelați să deschidă sau să descarce atașamente infectate, ceea ce duce la infectarea sistemului lor.

- Dispozitive de stocare externă: Virușii pot fi transferați de pe dispozitive de stocare externă, cum ar fi stick-urile USB sau discurile externe. Dacă aceste dispozitive conțin fișiere infectate, acestea pot infecta și alte sisteme atunci când sunt conectate.

- Vulnerabilități de securitate: Virușii pot profita de vulnerabilitățile de securitate ale sistemelor de operare sau ale altor software pentru a se răspândi și a infecta calculatoarele. Aceste vulnerabilități pot fi utilizate pentru a permite intrarea virușilor în sistem fără cunoștința utilizatorului.

2. Prezentati detaliat ciclul de viata a unui virus.

   Ciclul de viață al unui virus informatic poate fi împărțit în mai multe etape:

   - Faza de activare: Virusul este declanșat și își începe execuția. Aceasta poate fi inițiată de o acțiune specifică a utilizatorului, de un eveniment predefinit sau de o condiție specifică.

   - Faza de infectare: Virusul se atașează și se integrează în fișiere sau programe existente. Aceasta permite virusului să se răspândească atunci când fișierele infectate sunt deschise sau executate.

   - Faza de răspândire: Virusul începe să se răspândească în alte fișiere, programe sau sisteme. Acesta poate utiliza diferite metode de propagare, cum ar fi atașarea la e-mail-uri, infectarea dispozitivelor de stocare externă sau exploatarea vulnerabilităților de securitate.

   - Faza de acțiune: Virusul execută acțiunile malitioase pentru care a fost programat. Aceste acțiuni pot varia, de la ștergerea sau coruperea datelor, la blocarea accesului la fișiere sau la compromiterea securității sistemului.

   - Faza de ascundere: Virusul încearcă să se ascundă și să evite detecția. Acesta poate utiliza tehnici de criptare, mascare sau modificarea comportamentului pentru a evita să fie identificat și eliminat.

3. Prezentati cele doua categorii de virusi: distructivi si nedistructivi. Exemple.
    - Viruși distructivi: Acești viruși sunt programați să cauzeze daune și să distrugă sau să corupă fișierele sau sistemul informatic. Ei pot șterge date, bloca accesul la fișiere, corupe informații sau chiar să distrugă întregul sistem. Exemple de viruși distructivi includ "Melissa" care se răspândea prin intermediul e-mailului și afecta fișierele de pe computerele infectate, sau "ILOVEYOU" care era transmis sub forma unui fișier atașat și ștergea fișierele utilizatorilor infectați.

    - Viruși nedistructivi: Acești viruși nu cauzează daune imediate sistemului sau fișierelor, dar pot încărca resursele și pot afecta performanța generală a sistemului. Ei pot răspândi alte programe malware sau pot colecta informații personale fără consimțământul utilizatorului. Un exemplu de virus nedistructiv este "SpyEye" care monitorizează și fură informații financiare și bancare de pe sistemele infectate.

4. Caracterizaţi comportamentul virusilor de e-mail. Detaliati un exemplu.

Virusurile de e-mail reprezintă un tip comun de malware care se răspândește prin intermediul mesajelor de e-mail. Acestea pot avea diferite comportamente, inclusiv:

- Răspândirea în masă: Virusurile de e-mail pot fi programate să trimită automate mesaje infectate către o listă mare de adrese de e-mail. Aceste mesaje pot conține fișiere atașate infectate sau link-uri către site-uri web periculoase. Un exemplu de virus de e-mail care utilizează acest comportament este "WannaCry" care se răspândea rapid prin intermediul atașamentelor de e-mail și exploata vulnerabilități în sistemul de operare Windows.

- Spoofing (falsificare): Virusurile de e-mail pot falsifica adresele de expeditor pentru a părea că mesajele provin de la o sursă de încredere sau cunoscută. Acest lucru poate determina utilizatorii să deschidă mesajele sau să acceseze link-urile malware-ului. De exemplu, un virus de e-mail ar putea trimite mesaje care par să provină de la o bancă și să solicite utilizatorului să introducă informații confidențiale.

- Social Engineering (ingineria socială): Virusurile de e-mail pot folosi tehnici de manipulare psihologică pentru a induce utilizatorii să deschidă sau să acceseze conținutul infectat. Aceste mesaje pot crea un sentiment de urgență, să ofere recompense sau să pretindă că sunt legate de subiecte actuale sau de interes personal. Un exemplu este un e-mail care pretinde că ați câștigat o loterie și vă cere să descărcați un fișier pentru a primi premiul.

Curs 13

Programe antivirus -definitie, criterii de clasificare:

DEF: Software-urile antivirus sunt programe care încearcă să identifice, să neutralizeze sau să elimine o gama largă de amenințări, incluzând viermi, atacuri phishing, rootkits și troieni, colectiv descrișI ca malware.

Criteriile principale sunt:

- Protecție împotriva oricărei amenințări existentă într-un calculator
- Viteza de scanare a fișierelor
- Aptitudinea de a identifica amenințările necunoscute
- Aptitudinea de bloca tentativele de furt de date confidențiale(tehnica phishing)
- Protecție împotriva amenințărilor privind rețele publice și a internetului