



Ministerul Educației și Cercetării al Republicii Moldova
Centrul de Excelență în Informatică și Tehnologii Informaționale

"Aprob"



Directorul Centrului de Excelență în Informatică și
Tehnologii Informaționale

Vitalie Zavadschi

Curriculumul modular

P.04.A.036 Utilizarea algoritmilor de criptare a informației

Specialitatea: **61230 Rețele de calculatoare**
Calificarea: **Tehnician pentru rețele de calculatoare**

Chișinău, 2022



**Curriculumul a fost elaborat în cadrul
I.P. Centrul de Excelență în Informatică și
Tehnologii Informaționale**

Autor:

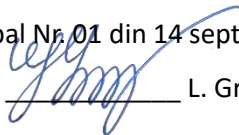
CERBU Olga, dr., conf. univ., grad didactic superior, Centrul de Excelență în Informatică și Tehnologii Informaționale.

Adoptat în baza Planului de învățământ, aprobat prin OMEC Nr.950/22, din 29.09.2022:

Dascăl Andrian, grad didactic doi, Centrul de Excelență în Informatică și Tehnologii Informaționale.

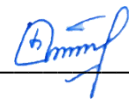
Examinat la ședința catedrei Informatică II

Proces verbal Nr. 01 din 14 septembrie 2022

Șef catedră  L. Gribineț

Aprobat de:

Consiliul metodic-științific al Centrului de Excelență în Informatică și Tehnologii Informaționale
Proces verbal Nr. 01 din 14 septembrie 2022

Director adjunct  Obadă Liuba

Recenzenți:

1. S.A. MoldTelecom, or. Chișinău, str. bd. Ștefan cel Mare, 10
2. Starnet Soluții S.R.L, or. Chișinău, str. Columna, 170

Cuprins

I. Preliminarii	4
II. Motivația, utilitatea modulului pentru dezvoltarea profesională	4
III. Competențele profesionale specifice modulului.....	5
IV. Administrarea modulului.....	5
V. Unitățile de învățare	6
VI. Repartizarea orientativă a orelor pe unități de învățare.....	8
VII. Studiu individual ghidat de profesor	8
VIII. Lucrările practice recomandate	9
IX. Sugestii metodologice	10
X. Sugestii de evaluare a competențelor profesionale.....	10
XI. Resursele necesare pentru desfășurarea procesului de studii.....	13
XII. Resursele didactice recomandate elevilor	13

I. Preliminarii

Securitatea informațională - un concept larg care cuprinde aproape orice software sau hardware conceput pentru a preveni pierderea sau furtul de date electronice - este important din mai multe motive, dar poate în principal ca mijloc de păstrare a informațiilor în siguranță. De cele mai multe ori, termenul „securitate informațională” se referă la securitatea datelor. Datele și informațiile compendioase pe care majoritatea utilizatorilor le stochează pe HDD-urile sau SSD-urile lor sunt adesea mult mai valoroase decât aparatele în sine. În linii mari, importanța securității informaționale constă în cât de dăunătoare poate fi dacă aceste date sunt pierdute sau deteriorate.

Majoritatea oamenilor se gândesc la securitatea informațională într-un context corporativ sau de afaceri. Companiile stochează adesea o mulțime de informații foarte sensibile pe cale electronică, inclusiv secrete comerciale, liste de clienți și documente corporative extinse, atât terminate, cât și cele în curs. Importanța securității datelor este evidentă în aceste contexte. Este probabil mai puțin evident pentru utilizatorii de computere de acasă, dar nu este mai puțin esențial.

Modulul „Utilizarea algoritmilor de criptare a informației” este o problemă vitală pentru toți utilizatorii de internet, fie că sunt furnizori de servicii, fie că sunt utilizatori simpli. Problemele de securitate care apar într-un sistem deschis, având în vedere sistemele ilegale, ce permit realizarea legăturilor logice (asociații) între utilizatorii rețelei prin excluderea politicii de autorizare și autentificare, a acceselor neautorizate, care permit unui utilizator sau proces autorizat, să acceseze obiecte la care nu are dreptul excluzând serviciile de control al accesului.

Una dintre soluțiile de bază de asigurare a asistenței în securitatea informației este metoda criptografică. Criptografia, la momentul actual, acoperă un set de protocoale, algoritmi de criptare, infrastructuri de manipulare a cheilor criptografice. Datorită progresului din tehnologia calculatoarelor asistența securității informației necesită proiectarea și analiza algoritmilor cu securitate condiționată să fie corelată cu definirea dificultății problemelor în teoria complexității.

Modulul “Asistență în securitatea informațională” este planificat pentru trei unități de învățare și este destinat căutării și stabilirii soluțiilor în asistența securității informației în cele mai diverse aspecte ale protejării ei de la aspectele legislative, la cele organizatorice, procedurale și funcționale.

Pentru a asigura cadrul teoretic necesar și aplicarea în dezvoltarea abilităților pentru protecția și securitatea informației este necesară studierea prealabilă a următoarelor unități de curs:

- P.01.O.010 Programarea calculatorului
- P.02.O.014 Asistența în administrarea serviciilor de rețea.

II. Motivația, utilitatea modulului pentru dezvoltarea profesională

Modulul “Utilizarea algoritmilor de criptare a informației” permite formarea abilităților practice de actualizare și utilizare a standardelor de securitate web prin utilizarea metodelor criptografice. Să cunoască formele de înșelăciuni pe Internet, scenarii de atacuri, să utilizeze instrumente, proceduri de diagnostică și metode de criptare pentru securizarea informației. Absolvenții prin parcurgerea integrală a modulului vor fi capabili să îndeplinească sarcini din conținutul de curs cu caracter teoretic și modalități de criptare în vederea atingerii competențelor vizate, cât și elaborarea produselor-program pentru implementarea în asistență în securitatea informațională.

Realizarea acestui modul presupune acumularea cunoștințelor și formarea abilităților în:

- Determinarea obiectului de studiu al disciplinei;

- Recunoașterea categoriilor de atacuri asupra metodelor de securitate;
- Cunoașterea nivelurilor, principiilor, politicilor și mecanismelor de securitate;
- Aplicarea cifrurilor clasice de substituție pentru securitatea informației;
- Elaborarea modului de implementare a asistenței în securitatea informației prin criptare în cadrul unui acces autorizat.
- Realizarea lucrărilor practice ale cursului presupune, în urma asimilării cunoștințelor predate în cadrul acestui modul, viitorul specialist își va putea asuma responsabilitatea punerii în funcțiune a diferitelor sisteme de securitate a informației și standarde de securitate.

Modulul asigură cadrul teoretic și practic necesar pentru dezvoltarea abilităților absolvenților la protecția și securitatea informațiilor cu cifruri clasice de substituție în asistența securității informației digitale.

III. Competențele profesionale specifice modului

Competențele profesionale ale viitorului absolvent evidențiază capacitatea de a integra cunoștințele teoretice cu deprinderile practice în realizarea activității profesionale și a obține performanțe descrise în calificarea profesională. Astfel modulul “Utilizarea algoritmilor de criptare a informației” conduce elevul la dobândirea competențelor profesionale specifice:

CS1. Instalează și configurează sisteme de securitate a sistemelor de calcul cu algoritmi de criptare.

CS2. Utilizează cifrurile clasice de substituție pentru securizarea sistemelor de calcul și a sistemelor informatice.

CS3. Utilizează metode de criptare eficiente și actuale contra diverselor forme de atac și fraude în mediul online și offline.

CS4. Crearea interfețelor la un nivel aplicativ cu metode de criptare asimetrice, simetrice pentru autentificarea și securizarea utilizatorilor.

IV. Administrarea modului

Modul de administrare a modului va fi redat în formă de tabel.

Semestrul	Numărul de ore				Modalitatea de evaluare	Numărul de credite
	Total	Contact direct		Lucrul individual		
		Prelegeri	Practică/ Seminar			
IV	90	20	40	30	Examen	3

V. Unitățile de învățare

Unități de competență	Unități de conținut	Abilități
1. Fundamentele securității informaționale.		
UC1. Identificarea și definirea conceptelor, teoriilor și metodelor folosite în realizarea de analize focusate pe protecția informației privind sistemele ce operează la nivel personal sau la nivel de organizații.	1. Concepte fundamentale privind securitatea informațională. - Scurtă istorie a securității informaționale. Principiile securității informaționale. - Nivelele de structurare a conceptului de securitate informațională. 2. Forme și tehnologii de manifestare a pericolelor în sistemele informaționale. - Amenințări și atacuri. Identificarea amenințărilor. Programe malițioase.	A1. Identificarea și definirea conceptelor, teoriilor, metodelor și principiilor aplicate în realizarea analizelor focusate pe protecția informației din perspectiva nivelelor de structură a viziunii securității informaționale. A2. Aplicarea mijloacelor software destinate administrării securității informaționale la nivel personal sau la nivel de organizații prin sisteme Backup, Restore, Recovery, antimalware și de fișiere cu jurnalizare.
2. Criptografie. Operații în criptografia aplicată.		
UC2. Identificarea operațiilor de multiplicare modulară prin descompunerea binară a exponentului, necesare pentru criptare și decriptare	1. Noțiuni fundamentale ale Criptografiei. - Clasificarea cifrurilor (sistemelor de criptare) după diverse criterii. Introducere în criptanaliză. 2. Operații în criptografia aplicată. - Operația de descompunere binară a exponentului în multiplicarea modulară. - Operația de determinare a inverselor elementelor dintr-un corp finit Z_n.	A3. Identificarea criteriilor fundamentale de clasificare a cifrurilor. A4. Aplicarea operației de exponențiere modulară la criptarea informației. A5. Aplicarea algoritmului lui Euclid extins pentru calculul inversei modulo în câmpul Z_n . A6. Utilizarea testelor de primalitate pentru generarea aleatoare a numerelor prime.

Unități de competență	Unități de conținut	Abilități
3. Cifruri clasice de substituție.		
UC3. Identificarea și definirea conceptelor cifrurilor clasice de substituție. UC4. Implementarea cifrurilor clasice de substituție prin operații de criptare și decriptare.	1. Cifruri clasice de substituție monoalfabetică. - Cezar, Afin, Polibios și ROT13 (Unix). Criptanaliza. 2. Cifruri clasice de substituție omofonică. 3. Cifruri clasice de substituție poligramică. - Playfair și Huffman. Criptanaliza. 4. Cifruri clasice de substituție polialfabetică. - Trithemius și Vigenere. Criptanaliza.	A7. Descrierea algoritmilor de criptare, decriptare pentru cifrurile clasice de substituție monoalfabetică. A8. Descrierea algoritmilor de criptare, decriptare pentru cifrurile clasice de substituție omofonică. A9. Descrierea algoritmilor de criptare, decriptare pentru cifrurile clasice de substituție poligramică. A10. Descrierea algoritmilor de criptare, decriptare pentru cifrurile clasice de substituție polialfabetică. A11. Criptanaliza cifrurilor clasice de substituție: monoalfabetică, omofonică, poligramică și polialfabetică.
4. Metode de criptare mod		
UC5. Implementarea sistemelor de criptare simetrică prin operații de criptare și decriptare. UC6. Implementarea sistemelor de criptare asimetrică prin operații de criptare și decriptare.	1. Sisteme de criptare simetrice: - AES. Operații de criptare, decriptare și criptanaliză a unui sistemului simetric. - DES. Operații de criptare, decriptare și criptanaliză a sistemului simetric. 2. Sisteme de criptare asimetrice: - RSA. Operații de criptare, decriptare și criptanaliză a sistemului asimetric. - Merkle-Hellman. Operații de criptare, decriptare și criptanaliză a sistemului asimetric.	A12. Descrierea algoritmilor de criptare, decriptare pentru sistemul de criptare AES. A13. Descrierea algoritmilor de criptare, decriptare pentru sistemul de criptare DES. A14. Criptanaliza sistemelor de criptare simetrice. A15. Descrierea algoritmilor de criptare, decriptare pentru sistemul de criptare RSA. A16. Descrierea algoritmilor de criptare, decriptare pentru sistemul de criptare Merkle-Hellman. A17. Criptanaliza sistemelor de criptare asimetrice.

VI. Repartizarea orientativă a orelor pe unități de învățare

Nr. crt.	Unități de învățare	Total Ore	Numărul de ore contact direct		Lucrul individual	Ore de contact direct după locul de instruire				
			Total	Contact direct		I/I		I/A		
				IT		IP	IT	IP	IT	IP
1.	Fundamentele securității informaționale.	8	6	2	4	2	-	-	2	4
2.	Criptografie. Operații în criptografia aplicată.	18	12	4	8	6	-	-	4	8
3.	Cifruri clasice de substituție.	36	24	8	16	12	-	-	8	16
4.	Metode de criptare moderne	28	18	6	12	10	-	-	6	12
	Total	90	60	20	40	30	-	-	20	40

VII. Studiu individual ghidat de profesor

Materii pentru studiul individual	Produse de elaborat	Modalități de evaluare	Termeni de realizare
1. Securitatea informației cu sisteme asimetrice			
1. Operația de descompunere binară a exponentului în multiplicarea modulară. 2. Operația de determinare a inverselor elementelor dintr-un corp finit Z_n .	Proiect individual 1: <i>Operații de bază în criptografia aplicată.</i>	Prezentare la calculator	Săptămâna a 4
2. Cifruri clasice de substituție			
1. Cifruri clasice de substituție monoalfabetică: Cezar, Afin, Polibios și ROT13 (Unix). 2. Cifruri clasice de substituție omofonică. 3. Cifruri clasice de substituție poligramică: Playfair și Huffman. 4. Cifruri clasice de substituție polialfabetică: Trithemius și Vigenere.	Proiect individual 2: <i>Criptarea, decriptarea și criptanaliza unui cifru clasic de substituție monoalfabetică și omofonică.</i> <i>Criptarea, decriptarea și criptanaliza unui cifru clasic de substituție polialfabetică și poligramică.</i>	Prezentare la calculator	Săptămâna a 8-10
3. Metode de criptare moderne			
1. Sisteme de criptare simetrice. 2. Sisteme de criptare asimetrice.	Proiect individual 3: <i>Criptarea, decriptarea și criptanaliza unui sistem de criptare modern.</i>	Prezentare la calculator	Săptămâna a 14-a

VIII. Lucrările practice recomandate

1. *Operație în criptografie aplicată.*

- Aplicarea operației de exponențiere modulară la criptarea informației. Realizați valoarea expresiei în aritmetica modulară: $x^c \bmod n$.
- Aplicarea algoritmului Euclid extins pentru calculul inversei modulo în câmpul Z_n . Realizați valoarea expresiei în aritmetica modulară: $b^{-1} \bmod n$.

2. *Securitatea informației cu cifrurile clasice de substituție monoalfabetică.*

- Realizați criptarea și decriptarea cu implementarea algoritmului Cezar. Parametri de lucru la alegere. Mesajul va conține simboluri din nume, prenume, vârstă și numărul de telefon.
- Realizați criptarea și decriptarea cu implementarea algoritmului Afin. Parametri de lucru la alegere. Mesajul va conține simboluri din nume, prenume, vârstă și numărul de telefon.
- Realizați criptarea și decriptarea cu implementarea algoritmului Polibios. Parametri de lucru la alegere. Mesajul va conține simboluri din nume, prenume, vârstă și numărul de telefon.
- Realizați criptarea și decriptarea cu implementarea algoritmului ROT13 (Unix). Parametri de lucru la alegere. Mesajul va conține simboluri din nume, prenume, vârstă și numărul de telefon.

3. *Securitatea informației cu cifrurile clasice de substituție omofonică.*

- Criptanaliza unui cifru de substituție omofonică. Parametri de lucru la alegere.
- Criptarea și decriptarea unui cifru de substituție omofonică. Mesajul va conține simboluri din nume, prenume, vârstă și numărul de telefon.

4. *Securitatea informației cu cifrurile clasice de substituție poligramică.*

- Realizați criptarea și decriptarea cu implementarea algoritmului Playfair. Parametri de lucru la alegere. Mesajul va conține simboluri din nume, prenume, vârstă și numărul de telefon.
- Realizați criptarea și decriptarea cu implementarea algoritmului Huffman. Parametri de lucru la alegere. Mesajul va conține simboluri din nume, prenume, vârstă și numărul de telefon.

5. *Securitatea informației cu cifrurile clasice de substituție polialfabetică.*

- Realizați criptarea și decriptarea cu implementarea algoritmului Trithemius. Parametri de lucru la alegere. Mesajul va conține simboluri din nume, prenume, vârstă și numărul de telefon.
- Realizați criptarea și decriptarea cu implementarea algoritmului Vigenere. Parametri de lucru la alegere. Mesajul va conține simboluri din nume, prenume, vârstă și numărul de telefon.

6. *Securitatea informației cu sistemele de criptare moderne*

- Realizați criptarea și decriptarea cu implementarea algoritmului AES. Parametri de lucru la alegere. Mesajul va conține simboluri din nume, prenume, vârstă și numărul de telefon.
- Realizați criptarea și decriptarea cu implementarea algoritmului DES. Parametri de lucru la alegere. Mesajul va conține simboluri din nume, prenume, vârstă și numărul de telefon.
- Realizați criptarea și decriptarea cu implementarea algoritmului RSA. Parametri de lucru la alegere. Mesajul va conține simboluri din nume, prenume, vârstă și numărul de telefon.
- Realizați criptarea și decriptarea cu implementarea algoritmului Merkle-Hellman. Parametri de lucru la alegere. Mesajul va conține simboluri din nume, prenume, vârstă și numărul de telefon.

IX. Sugestii metodologice

Curriculumul la modulul "Asistență în securitatea informațională" are drept scop formarea și dezvoltarea competențelor profesionale ale elevilor din învățământul profesional tehnic postsecundar. Securitatea informației este un concept mai larg care se referă la asigurarea integrității, confidențialității și disponibilității informației. Dinamica tehnologiei informației induce noi riscuri pentru care persoanele și în special organizațiile trebuie să implementeze noi măsuri de control. De exemplu, popularizarea unităților de înregistrare, Cloud-uri sau a memoriilor online de capacitate mare, induce riscuri de copiere neautorizată sau furt de date.

Se recomandă activitățile de instruire să aibă loc în săli echipate respectiv pentru îmbunătățirea instruirii interactive. La lecțiile de laborator este de recomandat ca fiecare elev să dispună de calculator echipat cu soft-urile necesare. Se propune utilizarea metodelor de predare-învățare activ-participative, din motivele următoare:

- Sunt orientate pe elev și activitate.
- Accentuează dezvoltarea gândirii, formarea aptitudinilor și a deprinderilor.
- Motivează participarea activă a elevilor, implicarea și creativitatea.
- Realizează comunicarea multidirecțională între profesor și elev.

Elaborarea proiectelor în cadrul activităților practice va urmări dezvoltarea abilităților de lucru colaborativ în echipă. Se vor selecta metode didactice cum ar fi: descoperire, discuția în grup, dezbateră/masa rotundă, studiul de caz, observația individuală.

Învățarea electronică sincronă este o învățare și predare online prin intermediul tehnologiilor de rețea, utilizând mijloace sincrone, cum ar fi videoconferință, mesagerie instantanee și chat. Permite elevilor și profesorilor să participe în timp real și să se implice în discuții sincron, similară unei ore organizată cu prezență fizică. Varietatea de activități care sunt acum accesibile on-line face posibilă crearea mai multor tipuri de medii de învățare eficiente, cum ar fi: un brainstorming interactiv în timp real, utilizarea unui conținut de înaltă calitate, care este disponibil on-line (tutoriale, video-uri, exerciții interactive, simulări și materiale suplimentare on-line). Se recomandă utilizarea unei singure platforme pentru a nu perturba concentrarea elevilor.

Specificul modulului impune metode didactice interactive, recomandând mai ales învățarea prin metode practice/activități de laborator, proiecte, portofoliul electronic. În studiu individual, se va axa pe studiere, analiza și sistematizarea materialului teoretic și practic în scopul îndeplinirii sarcinilor de lucru. Rezultatele activității individuale vor fi prezentate în formă de portofolii, proiecte, sarcini specifice.

X. Sugestii de evaluare a competențelor profesionale

Conform procesului de învățare-predare-evaluare pe competențe se presupune efectuarea evaluării pe parcursul întregului proces de instruire. Evaluarea continuă va fi structurată în evaluări formative și evaluări sumative (finale). Activitățile de evaluare vor fi orientate spre motivarea elevilor, cuantificarea și evidențierea succeselor, implementarea evaluării selective sau individuale. Procesul de evaluare va fi anunțat preventiv elevilor cât și aducerea la cunoștință tematica lucrărilor, modul de evaluare (bareme/grile/criterii de notare).

În tabelul de mai jos sunt prezentate produsele recomandate pentru evaluarea nivelului de dezvoltare a competențelor cognitive.

Nr. Crt	Produse pentru aprecierea competenței	Criterii de evaluare a produselor
1.	Un set de exerciții rezolvate (operații în criptografia aplicată realizate în aritmetica modulo.)	• Înțelegerea enunțului exercițiului. • Corectitudinea formulării ipotezelor. • Corectitudinea raționamentelor. • Corectitudinea testării ipotezelor. • Corectitudinea strategiei rezolutive. • Corectitudinea rezultatelor. • Modul de prezentare a rezultatelor. • Modul de interpretare a rezultatelor.
2.	Problemă rezolvată (crearea unui scenariu în care ambele părți utilizatorul A și B participă la rezolvarea problemei).	• Înțelegerea problemei. • Documentarea în vederea identificării informațiilor necesare în rezolvarea problemei. • Formularea și testarea ipotezelor. • Stabilirea strategiei rezolutive. • Prezentarea și interpretarea rezultatelor.
3.	Proiect elaborat (formularea problemei restricționată pentru realizarea protocoalelor de securitate dedicate).	• Validitatea proiectului - gradul în care acesta acoperă unitar și coerent, logic și argumentat tema propusă. • Completitudinea proiectului - felul în care au fost evidențiate conexiunile și perspectivele interdisciplinare ale temei, competențele și abilitățile de ordin teoretic și practic și maniera în care acestea servesc conținutului științific. • Elaborarea și structura proiectului - acuratețea, rigoarea și coerența demersului științific, logica și argumentarea ideilor, corectitudinea concluziilor. • Calitatea materialului folosit în realizarea proiectului, bogăția și varietatea surselor de informare, relevanța și actualitatea acestora, semnificația datelor colectate s.a. • Creativitatea - gradul de noutate pe care-l aduce proiectul în abordarea temei sau în soluționarea problemei.
4.	Rezumat oral (de preferat la temele care în condiții de laborator nu pot fi elaborate ca exemplu securitatea bazată pe codul genetic, criptografia cuantică).	• Expune tematica lucrării în cauză. • Utilizează formulări proprii, fără a distorsiona mesajul lucrării supuse rezumării. • Expunerea orală este concisă și structurată logic. • Folosește un limbaj bogat, adecvat tematicii lucrării în cauză. • Respectarea coeficientului de reducere a textului: 1/3 din textul inițial.
5.	Rezumat scris (se va recurge în cazul realizării numerice a schimbului exponențial de chei între doi utilizatori, pentru $n > 3$)	• Expune tematica lucrării în cauză. • Utilizează formulări proprii, fără a distorsiona mesajul lucrării supuse rezumării. • Textul rezumatului este concis și structurat logic.

Nr. Crt	Produse pentru aprecierea competenței	Criterii de evaluare a produselor
	utilizatori).	- Folosește un limbaj bogat, adecvat tematicii lucrării în cauză. - Fidelitatea: înțelegerea esențialului și reproducerea lui, nu trebuie să existe contrasens. - Coerența: rezumatul are o unitate și un sens evidente, lizibile pentru cei care nu cunosc textul sursă. - Progresia logică: înlănțuirea ideilor, prezentarea argumentelor sunt clare și evidente. - Angajamentul autorului, aptitudine critică corect evaluată și transpusă. - Respectarea modalităților de enunțare a textului sursă: rezumatul este o oglindă micșorată dar fidelă textului sursă. - Muncă pertinentă de reformulare: rezumatul nu este un colaj de citate. - Respectarea coeficientului de reducere a textului: 1/4 din textul inițial. - Stăpânirea normelor sintactice la nivel de prezentare logică a ideilor, frazelor, paragrafelor textului. Text formatat citeț, lizibil. plasarea clară în pagină.

Lista orientativă a categoriilor de produse și procese, recomandate pentru evaluarea competențelor funcțional-acționare este prezentată în tabelul de mai jos:

Nr. Crt	Produse pentru măsurarea competenței	Criterii de evaluare a produselor
1.	Elaborarea protocoalelor de criptanaliză cu realizare numerică și produs-program.	- Corespunderea termenilor de referință. - Corespunderea sarcinilor tehnice. - Corespunderea standardelor și normativelor în vigoare. - Corectitudinea calculelor. - Fundamentarea deciziilor. - Completitudinea setului de documente. - Ținuta lingvistică. - Respectarea termenilor de elaborare. - Productivitatea.

Pe parcursul modulului se realizează evaluare formativă prin aplicarea produselor pentru măsurarea competențelor cognitive și funcțional-acționare din tabelele de mai sus, iar la sfârșitul lui se realizează evaluarea sumativă pentru verificarea atingerii competențelor prin aplicarea unui test electronic.

XI. Resursele necesare pentru desfășurarea procesului de studii

Cerințe față de sălile de curs	
Pentru orele teoretice	- Cabinet de informatică cu 15 calculatoare - Tablă interactivă
Pentru orele de laborator	- Laborator de informatică care asigură fiecărui elev un calculator. - Tablă interactivă
Cerințe pentru lecții online	
Pentru orele de teorie, laborator	- Instrumente de comunicare sincronă - Platforme de colaborare online - Instrumente digitale de evaluare
Cerințe tehnice	
Parametri tehnici minimi ale calculatorului	- Procesor: 2 GHz - Memorie operativă: 4 GB - Unitate de stocare: 500 GB - Afișaj și grafică: dimensiune: 22'', rezoluția: 1366x768 - Rețea: Ethernet, 100 Mb
Software	- Sistem de Operare Microsoft Windows. - Eclipse Ed. 2020 - Visual Studio 2020. - Notepad++. - Browser: Chrome, FireFox

XII. Resursele didactice recomandate elevilor

Nr. crt.	Denumirea resursei	Locul în care poate fi consultată/ accesată resursa
1.	Codul Penal al Republicii Moldova. Capitolul al șaselea/1, infracțiuni în domeniul tehnologiilor informaționale.	www.gov.md
2.	Legea Republicii Moldova privind accesul la informație nr.982-XIV din 11.05.2000 //Monitorul Oficial al R. Moldova Nr.88-90/664 din 28.07.2000.	www.gov.md
3.	Zgureanu Aureliu, „Criptarea și securitatea informației”, 2013	http://dspace.ase.md:8080/xmlui/bitstream/handle/123456789/236/Zgureanu%20A.%20Criptarea%20%C5%9Fi%20Securitatea%20Informa%C5%A3iei.%20Note%20de%20curs.pdf?sequence=1&isAllowed=y
4.	A. Atanasiu, Criptografie, Editura InfoData, Cluj, 2008.	http://fmi.unibuc.ro/ro/pdf/2016/concursuri/Tematica_Info_Conf_31.pdf

Nr. crt.	Denumirea resursei	Locul în care poate fi consultată/ accesată resursa
5.	Iu. Căraș, O. Cerbu, V. Putină, Criptosisteme pe blocuri. Curs de lecții. Chișinău, Editura CEP, 2006.	books.google.md
6.	Чмора А. ,М. Гелиос, „Современная прикладная криптография “,2002.	books.google.md
7.	D. Stinson, Cryptography, Theory et Practice, Intern. Thompson Publ. House, Ed.I I(2002)	fmi.unibuc.ro/ro/pdf/2017/.../Tematica_concurs_conferentiar_28_Informatica_2017.pdf
8.	Adrian Constantin Atanasiu, Securitatea Informatiei vol 1 (Criptografie), 2009	https://www.researchgate.net/profile/Adrian-Atanasiu/publication/308791446_Securitatea_Informatiei_vol_1_Criptografie/links/57f1f67608ae280dd0b2804e/Securitatea-Informatiei-vol-1-Criptografie.pdf
9.	Adrian Constantin Atanasiu, Securitatea Informatiei vol 2 (Protocoale de securitate), 2009	https://www.researchgate.net/publication/308791369_Securitatea_Informatiei_vol_2_Protocoale_de_securitate/link/57f1f72a08ae91deaa56180a/download