Ministerul Educației și Cercetării al Republicii Moldova
Universitatea de Stat „Alecu Russo” din Bălți
Facultatea de Ştiinţe Reale, Economice şi ale Mediului
Catedra de matematică și informatică

Curriculum

la unitatea de curs

Securitatea sistemelor informatice

pentru studenţii de la specialitatea 0613.4 Informatică
Ciclul I, studii superioare de licență, învățământ cu frecvență

Autori:
Lidia POPOV, dr., conf. univ.
Alexandr PARAHONCO, asist. univ.

BĂLŢI, 2024

Discutat şi aprobat la şedinţa Catedrei de matematică şi informatică.

Procesul-verbal nr. 10 din 15 mai 2024.

Şeful Catedrei de matematică şi informatică _____ asist. univ. Vitalie ŢICĂU

Analizat şi recomandat la şedinţa Comisiei metodice a Facultăţii de Ştiinţe Reale, Economice şi ale Mediului.

Procesul-verbal nr. 7 din 05.06.2024.

Preşedintele Comisiei metodice al Consiliului Facultăţii de Ştiinţe Reale, Economice şi ale Mediului _____ conf. univ., dr. Lidia POPOV

Discutat şi aprobat la şedinţa Consiliului Facultăţii de Ştiinţe Reale, Economice şi ale Mediului.

Procesul-verbal nr. 11 din 10.06.24.

Decana Facultăţii de Ştiinţe Reale, Economice şi ale Mediului _____ conf. univ., dr. Ina CIOBANU

Informaţii de identificare a unității de curs

Facultatea: Științe Reale, Economice și ale Mediului

Catedra: Matematică și informatică

Codul și denumirea domeniului general de studiu: 061 Tehnologii ale informației și comunicațiilor

Codul și denumirea domeniului de formare profesională: 0613 Dezvoltarea produselor program și a aplicațiilor

Codul și denumirea specialității: 0613.4 Informatică

Administrarea unității de curs

Codul unității de curs	Nr. de credite ECTS	Total ore	Repartizarea orelor				Forma de evaluare	Limba de instruire
			Curs	Seminar	Laborator	Lucrul individual al studentului		
S.04A029	4	120	14	16	30	60	Examen	Română

Anul de studiu și semestrul în care se studiază: Anul II, Semestrul 4

Forma de organizare a învățământului: Învățământ cu frecvență

Regimul unității de curs: Unitate de curs opțională

Categoria formativă: Unitate de curs de specialitate

Informaţii referitoare la cadrele didactice

Titularul cursului: **Lidia POPOV**, conf. univ., doctor în științe ale educației la Catedra de matematică și informatică. A absolvit Universitatea de Stat din Moldova, Facultatea de Matematică şi Cibernetică, specialitatea „Matematica aplicată”. A obținut titlul de magistru în Informatică la Universitatea de Stat „Alecu Russo” din Bălţi. A susținut teza de doctor în științe ale educației la Universitatea de Stat din Tiraspol, cu sediul în municipiul Chişinău, Republica Moldova.

Domeniul de interes științific: Instruirea adaptivă în instituții de învățământ superior, utilizarea TIC în procesul didactic, didactica informaticii, învăţare electronică.

Biroul: Sala de calculatoare 545, Catedra de matematică și informatică

Telefon: 0-231-52-3-94; 0-231-52-4-88

E-mail: popov.lidia@usarb.md

Orele de consultaţii: Marţi 15:00-16:30. Consultațiile se oferă față în față, în cadrul grupului creat pe Viber, poștă electronică, videoconferință (Microsoft Teams, Google Meet, Zoom, Discord, Cisco Webex etc.).

Alexandr PARAHONCO, asist. univ. la Catedra de matematică și informatică. A absolvit Universitatea de Stat „Alecu Russo" din Bălți, Facultatea de Științe Reale, Economice și ale Mediului, specialitatea „Informatica și limba engleză". A obținut titlul de magistru în Informatică la Universitatea de Stat „Alecu Russo" din Bălţi, specialitatea „Programare Web". În prezent este doctorand la Universitatea „Alexandru Ioan Cuza" din Iaşi, specialitatea Informatica.

Domenii de interes științific: Programarea, Instruirea adaptivă în instituții de învățământ superior, utilizarea TIC în procesul didactic.

Biroul: Direcția Tehnologii Informaționale

Telefon: 0-231-52-3-82

E-mail: alexandr.parahonco@usarb.md

Orele de consultații: Joi, 15:00-16:30. Consultațiile se oferă față în față, în cadrul grupului creat pe Viber, poștă electronică, videoconferință (Microsoft Teams, Google Meet, Zoom, Discord, Cisco Webex etc.).

Integrarea unității de curs în programul de studii

Integrarea unității de curs *Securitatea sistemelor informatice* în programul de studii la specialitatea *Informatică* este esențială, având în vedere importanța crescută a securității informațiilor în era digitală actuală, în care datele și informațiile sunt expuse la diverse amenințări și riscuri de securitate și ar trebui să reflecte coerența și progresia adecvată a cunoștințelor și abilităților în domeniu. Legăturile cu alte unități de curs cum ar fi: *Proiectarea paginilor WEB, Bazele programării, Limbaje de programare structurată, Informatica generală, Sisteme de operare, Programare orientată pe obiect I, Programare funcțională/Programare logică, Gestiunea informației, Programare WEB I* pot consolida înțelegerea și aplicarea conceptelor securităţii sistemelor informatice într-un context mai larg și interdisciplinar.

Unitatea de curs menționată, include înțelegerea conceptelor și tehnicilor de securitate, identificarea și gestionarea riscurilor de securitate, cunoașterea standardelor și regulamentelor relevante etc. și este inclusă în planul de studiu al specialității *Informatică*, ca o materie opțională, în funcție de nivelul de importanță și complexitatea conținutului. Este structurată în patru compartimente, pre-

cum Curs, Seminar, Laborator, Lucrul individual al studentului care, la rândul său, acoperă diverse aspecte ale securității sistemelor informatice, cum ar fi securitatea rețelelor, securitatea bazelor de date, criptografia, gestionarea identității și accesului etc. Studenții au acces la resurse educaționale relevante, cum ar fi lecții, laboratoare plasate pe platforma de învățare MOODLE, manuale, instrumente software și alte materiale care să îi ajute să înțeleagă și să aplice conceptele de securitate în practică. Deoarece domeniul securității informatice este în continuă evoluție, unitatea de curs respectivă se actualizează în mod regulat pentru a reflecta cele mai recente amenințări, tehnologii și practici recomandate.

La această unitate de curs, studenții vor fi pregătiți să înțeleagă, să aplice și să gestioneze aspectele de securitate în domeniul lor de expertiză, contribuind astfel la securitatea și protecția informațiilor într-o lume digitală tot mai interconectată, totodată sunt orientați spre formarea și dezvoltarea competențelor digitale ce țin de securitatea sistemelor informatice în domeniul profesional.

Aceştia învață să identifice, să evalueze și să gestioneze riscurile de securitate în cadrul sistemelor informatice, precum și să dezvolte strategii și tactici eficiente pentru prevenirea și gestionarea incidentelor de securitate. De asemenea, sunt familiarizați cu diverse tehnologii și instrumente utilizate în securitatea sistemelor informatice, cum ar fi criptografia, firewall-urile, sistemele de detecție a intruziunilor, standardele și regulamentele relevante în domeniul securității informației etc.

Securitatea informatică nu se limitează doar la aspecte tehnice, ci implică și aspecte organizaționale, juridice și umane. Această abordare holistică este necesară pentru a asigura o securitate eficientă și durabilă a sistemelor informatice.

Prin intermediul lucrărilor de laborator, studenții au oportunitatea de a aplica conceptele și tehnologiile învățate în contexte reale, consolidând astfel cunoștințele lor și dezvoltându-și abilitățile practice în domeniul securității informatice.

Unitatea de curs *Securitatea sistemelor informatice* joacă un rol important în formarea studenților de la specialitatea *Informatică*, pregătindu-i să facă față provocărilor din domeniul securității informației și contribuind la asigurarea integrității, confidențialității și disponibilității datelor și informațiilor în era digitală.

Exigențe și competențe prealabile

Succesul în studierea unității de curs *Securitatea sistemelor informatice* depinde de un set variat de cunoștințe, abilități și atitudini dobândite anterior la unităţile de curs studiate, iar pregătirea și motivația studenților sunt esențiale pentru a face față provocărilor și complexității acestui domeniu. Este destul de important ca studenții să aibă anumite exigențe și competențe prealabile ce țin de cunoștințe de bază în informatică, fundamente matematice, abilități de programare, comunicare și gândire critică etc.

Studierea unității de curs menționate se bazează pe cunoştinţele, capacităţile şi competenţele dezvoltate în cadrul unităților de curs *Bazele programării*, *Structuri discrete, Proiectarea paginilor Web, Informatica generală* etc.

Competențe profesionale și transversale dezvoltate în cadrul unității de curs

În cadrul unității de curs *Securitatea sistemelor informatice*, studenții dezvoltă o serie de competențe profesionale și transversale esențiale pentru succesul lor în domeniul securității informațiilor. Prin conţinutul său şi activităţile de învăţare a studenţilor, această unitate de curs contribuie la dezvoltarea competenţelor digitale ce țin de securitatea sistemelor informatice în domeniul profesional precum: criptarea datelor; asigurarea schimbului de date securizat prin Firewall; crearea și configurarea serverului Proxy; setarea conexiunii securizate la distanță (VPN și DMZ); administrarea și securitatea sistemului de operare Windows etc.

Acest ansamblu de competențe servesc ca instrumente de formare atât a competențelor profesionale (CP), cât și a competențelor transversale (CT) vizate în planurile de învățământ la specialitatea menționată. Pe lângă competențele digitale necesare specialității respective nominalizate, unitatea de curs respectivă contribuie la dezvoltarea a mai multor competențe generice precum CP și CT necesare specialistului din domeniul profesional:

Competențe profesionale:

CP2. Proiectarea si realizarea unui demers de cercetare prin abilități de control și inovație în domeniul informaticii și tehnologiilor informaționale.

CP3. Identificarea, analiza, aprecierea critică a relațiilor de cauzalitate și interdependență dintre diferite evenimente, procese tehnice, fenomene socio-economice.

CP5. Proiectarea activităților de elaborare a produselor informatice, utilizând cunoștințele acumulate la studierea unităților de curs fundamentale și de specialitate.

Competențe transversale:

CT1. Aplicarea principiilor, normelor și valorilor eticii și deontologiei profesionale în cadrul propriei strategii de muncă, în situații specifice.

CT2. Desfășurarea eficientă și eficace a activităților organizate in echipă.

CT3. Identificarea oportunităților de formare continuă și valorificarea eficientă a resurselor și tehnicilor de învățare pentru propria dezvoltare.

Finalităţile unității de curs

La finalizarea studierii unității de curs *Securitatea sistemelor informatice* și realizarea sarcinilor de învățare, studentul va fi capabil:

– să cripteze datele și să asigure schimbul de date securizat prin FIREWALL;
– să creeze și să configureze serverului PROXY;
– să seteze conexiunile securizate la distanță (VPN și DMZ);
– să administreze și să securizeze sistemul de operare Windows;
– să asigure securitatea utilizării calculatorului;
– să asigure securitatea rețelelor de calculatoare.

Conținutul unității de curs

a) Curs – 14 ore

Nr. d/o	Subiectele de studiu	Nr. de ore
1.	Noţiuni privind securitatea informaţiilor.	2
2.	Clasificarea informaţiilor.	2
3.	Controlul accesului în sistemele informatice.	2
4.	Criptografia. Modele şi programe de securitate.	2
5.	Evaluarea periodică	2
6.	Securitatea reţelelor de calculatoare.	2
7.	Tehnici, servicii şi soluţii de securitate pentru intranet-uri şi portaluri. Strategii de achiziţie pentru apărare.	2
Total		**14**

b) Seminar – 16 ore

Nr. d/o	Subiectele de studiu	Nr. de ore
1.	Noţiuni privind securitatea informaţiilor.	2
2.	Clasificarea informaţiilor.	2
3.	Controlul accesului în sistemele informatice.	2
4.	Criptografia.	2
5.	Modele şi programe de securitate.	2
6.	Securitatea reţelelor de calculatoare.	2
7.	Tehnici, servicii şi soluţii de securitate pentru Intranet-uri şi Portaluri.	2
8.	Strategii de achiziţie pentru apărare.	2
Total		**16**

c) Laborator – 30 de ore

Nr. d/o	Subiectele de studiu	Nr. de ore
1.	Criptarea ca metodă de securitate a informaţiilor.	4
2.	Steganografia ca metodă de securitate a informaţiilor.	4
3.	Firewall-uri.	4
4.	Proxy Server.	4

Nr. d/o	Subiectele de studiu	Nr. de ore
5.	Proxy Server Squid.	4
6.	Open VPN.	4
7.	Utilizatori și grupuri Windows. Securitatea accesului.	4
8.	*Evaluarea Lucrului individual.*	2
Total		**30**

Subiectele de studiu la lucrările de laborator, reflectate în tabel, sunt însoţite de materialul teoretic corespunzător. Studenţii, înainte de a efectua o lucrare de laborator, studiază materialul teoretic respectiv plasat în diverse locuri disponibil tuturor: platforma de învățare MOODLE; poșta electronică comună a grupei academice etc. Aceștia îndeplinesc lucrările de laborator conform indicaţiilor metodice şi le prezintă profesorului în termenul stabilit. Din start, studenții sunt înscriși la unitatea de curs *Securitatea sistemelor informatice* plasată pe platforma de învățare MOODLE de către Direcția Tehnologii Informaționale (DTI) al Universității de Stat „Alecu Russo” din Bălți și au acces liber la cursul respectiv și la toate materialele aferente acestuia. Printre aceste materiale sunt incluse activităţi interactive, lucrări de laborator însoțite de diverse cerinţe, temele pentru lucrul individual etc.

Strategii de predare și învățare

Pentru a asigura o învățare eficientă în cadrul unității de curs *Securitatea sistemelor informatice*, se utilizează strategii de predare și învățare variate și adaptate nevoilor și stilurilor de învățare ale studenților precum: metode interactive de predare; utilizarea tehnologiei și a resurselor online; dezbaterea și colaborarea în echipă; feedback și evaluare formativă; legătura cu aplicațiile practice; dezvoltarea de proiecte practice; folosirea resurselor multimedia, lucrarea de laborator etc.

Lucrarea de laborator este o strategie de învățare valoroasă în cadrul unității de curs *Securitatea sistemelor informatice*, oferă studenților oportunitatea de a aplica cunoștințele teoretice într-un mediu practic și de a dezvolta abilități practice esențiale în domeniul securității informațiilor. Permit studenților să aplice conceptele teoretice în soluționarea problemelor practice din domeniul securității sistemelor informatice, facilitează înțelegerea mai profundă și mai concretă a subiectului, oferă oportunitatea de a învăța prin experiență directă, permițând studenților să experimenteze, să testeze și să exploreze diferite scenarii și soluții într-un mediu controlat și sigur.

Lucrările de laborator stimulează gândirea critică și creativă a studenților, punându-i în fața unor provocări și probleme complexe de securitate pe care trebuie să le rezolve prin abordări inovatoare și soluții originale.

Prin intermediul lucrărilor de laborator, studenții pot consolida cunoștințele și abilitățile dobândite în cadrul cursului, permițându-le să-și pună în aplicare în mod practic înțelegerea și să-și îmbunătățească competențele în domeniul securității informațiilor.

Prin utilizarea acestor strategii de predare și de învățare în cadrul cursului *Securitatea sistemelor informatice*, se creează un mediu de învățare stimulativ și eficient, care să încurajeze implicarea și să faciliteze atât dezvoltarea competentelor profesionale, cât și transversale esențiale pentru studenții din domeniul securității informațiilor.

Activităţi de lucru individual al studentului

Activitățile de lucru individual al studentului prezintă o componentă importantă, obligatorie a procesului de învățare și pot fi folosite în cadrul cursului *Securitatea sistemelor informatice* pentru a promova înțelegerea profundă, dezvoltarea abilităților și îmbunătățirea performanței academice, include studiul după manualele recomandate și suportul de curs oferit de către titularul cursului. Studenților li se propune o listă cu diverse teme din domeniul securității sistemelor informatice pentru elaborarea unui proiect individual care, la rândul său, presupune verificarea competențelor dezvoltate la unitatea de curs menţionată. Cerinţele de elaborare a proiectului sunt plasate pe platforma de învățare MOODLE încadrate în cursul respectiv. Fiecare student din grupa academică, alege o temă la dorință, o temă unică, la care lucrează pe tot parcursul semestrului, demonstrând competențele dobândite în domeniul securității informațiilor.

Criteriile de evaluare a proiectului sunt următoarele:

– tehnoredactarea documentului la cele trei nivele;
– integrarea în proiect a resurselor elaborate la temele studiate;
– desfășurarea temei selectate;
– prezentarea și expunerea temei selectate etc.

Rezultatele obținute ale activităților individuale, studenții le prezentă public, la finele semestrului (la ultima lecție de Laborator) și vor fi notați cu notă (**I** – lucrul individual).

Evaluarea

Evaluarea cunoștințelor la unitatea de curs *Securitatea sistemelor informatice*, se realizează în corespundere cu Regulamentul de organizare a studiilor superioare de licență (Ciclul I) în Universitatea de Stat „Alecu Russo” din Bălți și cu Regulamentul-cadru privind evaluarea cunoştinţelor studenţilor, obţinute în procesul de formare şi a rezultatelor academice ale acestora.

Cunoştinţele, abilitățile şi competențele studenţilor vor fi evaluate pe parcursul semestrului (evaluarea curentă) și la finele semestrului (evaluarea finală). Evaluarea curentă se efectuează la

seminare prin răspunsuri orale, participare la discuții și soluționarea sarcinilor la lucrările de laborator, susținând fiecare lucrare în parte și fiind apreciat cu notă.

Media evaluării curente reprezentă o medie calculată din minimum patru note de la Seminar și 7 note de la Laborator (7 Lucrări de laborator).

Evaluarea periodică se organizează după predarea a circa jumătate din orele de curs și cel puțin 1/3 din orele practice preconizate pentru unitatea de curs menționată. Titularul de curs anunță la începutul semestrului temele în baza cărora vor fi formulate subiectele pentru evaluarea periodică. Evaluarea periodică se realizează în scris în cadrul orelor de contact direct. Studenții care absentează și cei care obțin o notă mai mică decât 5, susțin repetat testul de evaluare periodică conform orarului.

La evaluarea finală sunt admiși doar studenții care întrunesc următoarele condiții:

– media notelor evaluărilor curente $\mathbf{M_c}$ este de cel puțin 5;
– nota la evaluarea periodică $\mathbf{N_p}$ este de cel puțin 5;
– nota pentru activitatea individuală **I** este de cel puțin 5.

Nota semestrială ($\mathbf{N_s}$) se calculează ca media aritmetică a trei componente: Media notelor evaluărilor curente ($\mathbf{M_c}$), Nota la evaluarea periodică ($\mathbf{N_p}$) și Nota pentru activitatea individuală (**I**):

$$N_s = \frac{M_c + N_p + I}{3}.$$

Media semestrială constituie 60% din nota generală la unitatea de curs, celelalte 40% le constituie nota de la examen. Evaluarea finală este realizată sub forma unui examen în scris. Durata examenului nu este mai mică de 3 ore.

Nota generală la unitatea de curs *Securitatea sistemelor informatice* se calculează (cu două cifre zecimale după virgulă) conform formulei:

$$\mathbf{N_g} = 0.6 \cdot N_s + 0.4 \cdot N_e,$$

unde $\mathbf{N_g}$ este nota generală, $\mathbf{N_s}$ este nota semestrială și $\mathbf{N_e}$ este nota de la examen.

La finalizarea studierii unității de curs, studentul evaluează prin completarea anonimă a unui chestionar în variantă electronică atât unitatea de curs, cât și cadrul didactic, în scopul îmbunătăţirii procesului de instruire la unitatea de curs menționată.

MODEL DE TEST DE EVALUARE PERIODICĂ

Completează (3 p)

1. Cele trei atribute ale securității informatice sunt

a. b. c.

Completează (5p)

2. Secțiunile standardului de securitate ISO/IEC 17799 se numesc _____

_____

Completează (5 p)

3. Principiile protejării informațiilor speciale sunt _____

_____

Completează (3 p

4. Combinaţiile obținute prin combinarea *controlului preventiv* şi *detectiv* cu mijloacele celorlalte tipuri de control: administrativ, logic şi fizic÷ sunt _____)

Completează (1 p)

5. Criptografia prezintă _____

Completează (1 p)

6. Steganografia prezintă _____

7. Criptează mesajul „MODUL SISTEM SUPERIOR”, utilizând cheia 15-6-10 și alfabetul (6 p)

Tabel 1.Alfabet român

A	Ă	Â	B	C	D	E	F	G	H	I	Î	J	K	L	M	N	O	P	Q	R	S	Ș	T	Ț	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Cuvântul: MODUL

Cheia										
Mesaj										
Poziția										
Poziția criptată										
Mesaj Criptat										

Cuvântul: SISTEM

Cheia											
Mesaj											
Poziția											
Poziția criptată											
Mesaj Criptat											

Cuvântul: SUPERIOR

Cheia											
Mesaj											
Poziția											
Poziția criptată											
Mesaj Criptat											

8. Decriptează mesajul „ÂNÎJK TDÎXBEI”, utilizând cheia PZE și alfabetul român (4 p)

Cuvântul: ÂNÎJK

Cheia											
Mesaj Criptat											
Poziția criptată											
Poziția											
Mesaj											

Cuvântul: TDÎXBEI

Cheia											
Mesaj Criptat											
Poziția criptată											
Poziția											
Mesaj											

Încercuiește numărul răspunsului corect

9. Rețeaua care permite inițial partajarea resurselor este (1 p)

1. rețeaua de acasă (домашняя сеть);
2. rețea de întreprindere (сеть предприятия);
3. rețea publică (общественная сеть).

Citește afirmația de mai jos. Dacă consideri că afirmația este adevărată, încercuiește litere **A**, în caz contrar, încercuiește litera **F**.

10. **A F** În cazul în care opțiunea „Descoperirea rețelei” la rețeaua respectivă este bifată, două calculatoare conectate la o rețea comună pot să acceseze resursele comune.

Baremul de notare

Nota	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Puncte	0-1	2-3	4-5	6-9	10-14	15-18	19-23	24-27	28-29	30

MODEL DE TEST DE EVALUARE FINALĂ

Completează (3 pt)

1. ISO/IEC 17799 tratează securitatea informaţiilor prin prisma a trei elemente principale:

a. b. c.

Completează (2 pt)

2. Cele două strategii de bază privind securitatea naţională sunt

a. b.

Completează (5 pt)

3. Principiile protejării informațiilor speciale se numesc

Completează (3 pt)

4. Tipurile de control al accesului în sistemul informațional sunt

a. b. c.

Completează (1 pt)

5. Steganografia prezintă

Completează (1 pt)

6. Cifrul lui Cezar prezintă

Completează (3 pt)

7. Cele mai cunoscute modele de politici de securitate sunt

Completează (1 pt)

8. Criptografia prezintă _____

9. (3 pt) Steganografia cu imagini. O imagine cu **370676** de pixeli. **Calculează** numărul maximal de **biți** și **caractere** care pot fi ascuns într-o această imagine, utilizând metodologie

✓ cu 3 culori; ✓ cu 2 culori; ✓ cu o culoare.

10. **Efectuează următoarele calcule:**

(2 pt) **Server Squid**. Definește regulile **acl** și **aplic**ă-le:

1. preveniți acces pentru IP 192.168.20.8 cu masca 255.255.255.0
2. dați acces Luni – Vineri de la 08:30 până la 17:30.

Regulile acl **Aplicarea regulilor acl**

1)

2)

11. (6 pt) **Cifrul lui Cezar**. Criptează mesajul „PROXY SERVER SQUID” cu cheia FOȚZ și alfabetul român. Prezentă calculele.

Alfabet român																													
A	Ă	Â	B	C	D	E	F	G	H	I	Î	J	K	L	M	N	O	P	Q	R	S	Ș	T	Ț	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Barem de notare

Nota	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Puncte	0-1	2-3	4-5	6-9	10-14	15-18	19-23	24-27	28-29	30

Resurse informaționale

1. ANDERSON, R. *Securitatea informației: O introducere*. Chișinău: Editura Arc, 2019, 592 p. ISBN 978-9975-55-362-5.
2. ANDERSON, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*, New York, USA: Wiley, 2001, 1080 p. ISBN 978-047-006-852-6.
3. ANDERSON, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Indianapolis, USA: Wiley, 2019, 1080 p. ISBN 978-111-965-091-6.
4. ANDRESS, M. *Surviving Security: How to Integrate People, Process and Technology.* Indianapolis, USA: SAMS Publishing, 2002, 288 p. ISBN 978-067-232-249-6.
5. BOGDAN, D., CÎRLUGEA, D. *Criptografia și securitatea rețelelor*. București: Editura Universității din București, 2015 , 226 p. ISBN 978-606-16-0626-7.
6. EZRA, P., MISRA, S., AGRAWAL, A., OLURANTI, J., MASKELIUNAS, R., & DAMASEVICIUS, R. *Secured communication using virtual private network (VPN).* In: *Cyber Security and Digital Forensics: Proceedings of ICCSDF, 2022*, pp. 309-319. ISBN: 978-981-16-3960-9. DOI: 10.1007/978-981-16-3961-6_27
7. FILIP, F., FURTUNĂ, A., ISTRATE, G. *Securitatea informației și criptografia*. București: Editura Printech, 2018, 358 p. ISBN 978-606-938-348-3.
8. HAYAKAWA, Y., Honda, M., Santry, D., & Eggert, L. Prism: Proxies without the pain. In: *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, 2021, p. 535-549. ISBN 978-1-939133-21-2
9. KAUFMAN, C. PERLMAN, R., SPECINER, M. *Securitatea rețelelor: Comunicare privată într-o lume publică*. Chișinău: Editura C-TEC Press, 2017, 752 p. ISBN 978-9975-63-213-8.
10. LEEUW, K., MAESENEER, E., BRAND, M. *The History of Information Security: A Comprehensive Handbook*. Amsterdam, Netherlands: Elsevier, 2007, ISBN 978-044-4516-507.
11. MARINESCU, D. *Securitatea și criptografia rețelelor de calculatoare*. București: Editura Matrix Rom, 2017, 288 p. ISBN 978-606-25-0514-4.
12. MIHAILESCU, M. *Securitatea informatică în rețele de calculatoare*. Iași: Editura Polirom, 2016, 376 p. ISBN 978-973-46-6141-4.
13. MONTE, M., MELVIN, M. FELDMAN, J. *Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats*. Boston, USA: Syngress, 2014, 320 p. ISBN 978-012-419-967-2.
14. MONTE, M., MELVIN, M., FELDMAN, J. *Construirea unui program de conștientizare a securității informațiilor: Apărându-vă împotriva ingineriei sociale și a amenințărilor tehni-*

ce. Editura: Polirom, Chișinău, 2017, 320 p. ISBN 978-9975-16-149-9. Editura Polirom este la Iași. Căutarea în Internet nu arată această sursă

15. PACHGHARE, V. K. Cryptography and information security. *PHI Learning Private Limited*. Delhi, 2019. ISBN: 978-93-89347-11-1
16. PECA, L., & Țurcanu, D. *Network security: Practical examples solved to be introduced in network security*. Chișinău: Editura Tehnica UTM, 2023. ISBN: 978-9975-45-941-9
17. PFLEEGER, C., PFLEEGER, Sh., MARGULIES, J. *Security in Computing*. Boston, USA: Pearson, 2015, 944 p. ISBN 978-013-408-504-3.
18. SCHNEIER, B. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, USA: W. W. Norton&Company, 2015, 400 p. ISBN 978-039-324-481-0.
19. SCHNEIER, B. *Data și Goliath: Lupta ascunsă pentru colectarea datelor tale și controlul lumii*. București: Editura publică, 2019, 440 p. ISBN 978-606-722-405-5.
20. SCHNEIER, B. *Securitate totală: Protecție maximă pentru Internet și rețele*. Chișinău: Editura Tehnica Info, 2016, 320 p. ISBN 978-9975-45-398-6.
21. SHOSTACK, A., STEWART, A. *Threat Modeling: Designing for Security*. Indianapolis, USA: Wiley, 2014, 624 p. ISBN 978-111-880-999-0.
22. STALLINGS, W. *Criptografia și securitatea rețelelor: Principii și practici*. Chișinău: Editura ExLibris, 2018, 752 p. ISBN 978-9975-52-951-4.
23. ИВАНОВ, И. *Базовые принципы информационной безопасности*. Москва: Издательство Техника, 2018, 320 с. ISBN 978-5-17-114159-3.

Principii de lucru în cadrul unității de curs

1. Fiecare oră va începe cu un scurt rezumat al temei predate anterior, timp de 5 minute.
2. Este salutată poziţia activă a studentului care studiază din propria iniţiativă noi conţinuturi, propune soluţii (aplicaţii, instrumente Web etc.), formulează întrebări în cadrul prelegerilor, seminarelor şi a orelor de laborator.
3. In cadrul unității de curs *Securitatea sistemelor informatice* o atenție sporită va fi oferită respectării principiilor etice. Prezentarea unor soluții a sarcinilor, preluate de la colegi sau din alte surse, preluarea informațiilor din diverse surse, fără a face trimitere la sursă, va fi considerată plagiat și va fi sancționată prin note de „1”.
4. În cazul în care studentul lipsește de la ore, acesta este obligat să efectueze toate lucrările de laborator la care a lipsit și să le susțină conform orarului consultațiilor curente la unitatea de curs nominalizată, în afara orelor de curs.
5. În cazul în care studentul lipsește de la ore mai mult de 30% din orele repartizate la unitatea de curs, el nu este admis la proba de evaluare finală, în conformitate cu regulamentul în vigoare, despre evaluare la Universitatea de Stat „Alecu Russo” din Bălți.
6. Nu este salutată întârzierea la ore.