

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
UNIVERSITATEA DE STAT „ALECU RUSSO” DIN BĂLȚI
FACULTATEA DE ȘTIINȚE REALE, ECONOMICE ȘI ALE MEDIULUI
CATEDRA DE MATEMATICĂ ȘI INFORMATICĂ

Curriculum pentru unitatea de curs
Gestiunea securității informației

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

Programul de master: Administrarea bazelor de date și tehnologii Web (120 credite)

Programare Web (120 credite)

Ciclul II, studii superioare de master, învățământ cu frecvență

Autori:

Lidia POPOV, dr., lect. univ.

Sergiu CHILAT, lect. univ.

Curriculum-ul la unitatea de curs *Gestiunea securității informatice* a fost discutat la ședința Catedrei de matematică și informatică.

Procesul-verbal nr. 12 din 15 iunie 2021.

Șeful Catedrei  dr., conf. univ. Corina NEGARA

Curriculum-ul la unitatea de curs *Gestiunea securității informatice* a fost aprobat la ședința Consiliului Facultății de Științe Reale, Economice și ale Mediului.

Procesul-verbal nr. 12 din 16 iunie 2021.



Decanul Facultății  dr., conf. univ. Ina CIOBANU

Informații de identificare a unității de curs

Facultatea: Științe Reale, Economice și ale Mediului

Catedra: Matematică și informatică

Codul și denumirea domeniului fundamental al științei, culturii și tehnicii: 06 Tehnologii ale informației și comunicațiilor

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

Programul de studii la ciclul II, studii superioare de master: Administrarea bazelor de date și tehnologii WEB, Programare WEB

Titlul conferit la absolvirea ciclului II, studii superioare de master: Master în Informatică

Administrarea unității de curs

Codul unității de curs	Credite ECTS	Total ore	Repartizarea orelor				Forma de evaluare	Limba de predare
			Prelegeri	Seminare	Laborator	Lucrul individual		
S.02.O.110	5	150	24	0	16	110	Examen	Română/ Rusă

Anul de studiu și semestrul în care se studiază unitatea de curs: Anul I, Semestrul 1

Forma de organizare a învățământului: cu frecvență

Regimul unității de curs (obligatorie/opțională/la liberă alegere): Obligatorie

Statutul: Unitate de curs de specialitate

Informații referitoare la titularul de curs și cadrele didactice implicate



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

Domeniul de interes științific: Instruirea adaptivă în instituții de învățământ superior, utilizarea TIC în procesul didactic, didactica informaticii, învățare 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 consultații: Marți 15:00 – 16:30. Consultațiile se oferă față în față, în cadrul grupului creat pe Viber, poștă electronică, videoconferință (aplicația Google Meet, Zoom, Discord).



Orele de laborator: **Sergiu CHILAT**, asistent universitar la Catedra de matematică și informatică. A absolvit Universitatea de Stat „Alec Russo” din Bălți, specialitatea „Matematică și informatică”. A obținut titlul de magistru în Informatică la Universitatea de Stat „Alec Russo” din Bălți. Studii de doctorat la Universitatea Tehnică a Moldovei. Activează în funcția de Director tehnic la compania Power IT SRL.

Domeniul de interes științific: Tehnologii Cloud

Biroul: Sala de calculatoare 150, Catedra de matematică și informatică

Telefon: 0-231-52-4-88

E-mail: chilatsergiu@gmail.com

Orele de consultații: Miercuri, 15:00 – 16:30: Consultațiile se oferă față în față, în cadrul grupului creat pe Viber, Skype, poștă electronică, videoconferință (aplicația Google Meet, Zoom).

Integrarea cursului în programul de studii

Unitatea de curs *Gestiunea securității informatice* se predă în Anul I de studii, Sem. 1 la specialitățile *Administrarea bazelor de date și tehnologii Web* și *Programare Web*.

Cursul respectiv este orientat spre înțelegerea, organizarea și asigurarea securității informațiilor unei Unități Social Economice (USE), pornind de la cerințele pentru Sistemul de Management al Securității Informațiilor (SMSI), specificate în ISO/IEC 27001, analiza contextului organizației, stabilirea SMSI, identificarea și analiza riscurilor, alegerea măsurilor de asigurare a protecției informațiilor și terminând cu monitorizarea SMSI conform ciclului PDCA.

Unitatea de curs *Gestiunea securității informatice* este una de specializare care permite aprofundarea cunoștințelor în programare. Realizarea unui sistem informatic reprezintă o activitate complexă și de durată, ce antrenează mari resurse materiale, umane și de timp. Securitatea informației se ocupă de protejarea informației și a sistemelor informatice de accesul neautorizat, folosirea, dezvăluirea, întreruperea, modificarea or distrugerea acestora. ISO/IEC27002/2013 tratează securitatea informațiilor prin cele trei componente principale: confidențialitatea, integritatea și disponibilitatea. *Confidențialitatea* este asigurată prin criptarea informației. *Integritatea* se obține prin mecanisme și algoritmi de dispersie. *Disponibilitatea* asigură prin întărirea securității rețelei sau rețelelor de sisteme informatice și asigurarea de copii de siguranță. În cadrul unității de curs

respective se studiază noțiuni de: securitate, autentificare, autorizare, confidențialitate, politica de securitate, drepturile de autor etc. Viitorii profesioniști vor obține cunoștințe referitor la diverse modalități de securitate a aplicațiilor software.

Studierea unității de curs *Gestiunea securității informatice* se sprijină pe cunoștințele, capacitățile și competențele dezvoltate în cadrul unității de curs *Programarea obiect orientată, Arhitectura calculatoarelor și sisteme de operare, Baze de date, Programarea Web, Rețele de calculatoare*, studiate la Ciclul I, licență. Finalitățile și conținutul unității de curs sunt corelate cu finalitățile și conținuturile unităților de curs menționate mai sus.

Unitatea de curs respectivă fiind una obligatorie la ambele specialități din cadrul facultății ȘREM a Universității de Stat „Alec Russo” din Bălți, are drept scop formarea și dezvoltarea la studenți a competențelor digitale ce țin de securitatea informației în domeniul profesional.

Competențe prealabile

Studierea unității de curs *Gestiunea securității informatice* se bazează pe cunoștințele, capacitățile și competențele dezvoltate în cadrul următoarelor unități de curs studiate la Ciclul I, licență:

1. Programarea orientată pe obiect: Clase. Moștenire. Polimorfism. Obiecte.
2. Arhitectura calculatoarelor și sisteme de operare: componentele calculatoarelor, sistemele de operare Windows, Linux.
3. Gestiunea informației: SGBD, proiectarea bazelor de date.
4. Programarea Web: client, server, site etc.

De asemenea, se bazează și pe competențele formate prin studierea în semestrul I a cursului *Securitatea informației întreprinderilor*.

Competențe dezvoltate în cadrul cursului

Prin conținutul său și activitățile de învățare a studenților, unitatea de curs *Gestiunea securității informatice* contribuie la dezvoltarea competențelor digitale necesare viitorului specialist în domeniul profesional. La rândul său, ansamblul de competențe servesc ca instrumente de formare a competențelor profesionale (CP) și a competențelor transversale (CT) vizate în planurile de învățământ la specialitățile nominalizate.

Pe lângă competențele digitale necesare diverselor specialități enumerate atât în *Standardele de eficiență a învățării*, cât și în *Standardele de competențe digitale pentru cadrele didactice din învățământul general* unitatea de curs *Gestiunea securității informatice* contribuie la dezvoltarea a mai multor competențe generice atât CP, cât și CT, necesare specialistului din domeniul profesional.

a) Competențe profesionale:

CP1. Utilizarea creativă a cunoștințelor fundamentale și avansate, a metodelor moderne din informatică, TIC în activitățile specifice domeniului și în comunicarea profesională.

CP2. Utilizarea tehnologiilor, echipamentelor și aplicațiilor informatice destinate gestionării activității profesionale.

CP3. Proiectarea, elaborarea și analiza modelelor/algoritmilor pentru rezolvarea problemelor.

CP4. Programarea, dezvoltarea și mentenanța aplicațiilor informatice în limbaje de nivel înalt.

CP6. Gestionarea, prelucrarea, analiza și interpretarea bazelor de date.

b) Competențe transversale:

CT1. Aplicarea regulilor de muncă riguroasă și eficientă, manifestarea unei atitudini responsabile față de domeniul științific și de producere, pentru valorificarea optimă și creativă a propriului potențial în situații specifice, cu respectarea principiilor și a normelor de etică profesională.

CT2. Identificarea rolurilor și responsabilităților într-o echipă plurispecializată, luarea deciziilor și atribuirea de sarcini, cu aplicarea tehnicilor relaționare și muncă eficientă în cadrul echipei.

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

Finalitățile unității de curs

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

- să identifice principalele concepte, principii, modele și tehnici de aplicare relative la securitatea informațională;
- să utilizeze cunoștințele în gestiunea a securității unor componente software și hardware;
- să implementeze soluții de securitate folosind diverse tehnologii actuale;
- să evalueze și analizeze securitatea unui sistem informațional;
- să determine resurselor necesare realizării securității informațiilor;
- să analizeze atributele măsurabile ale securității informațiilor;
- să identifice modurile de elaborare a politicii de securitate în cadrul unei organizații;
- să proiecteze și să aplice setul de măsuri care vor asigura securitatea informației etc.

Conținuturi

Prelegeri (24 de ore)

Nr. d/o	Subiectele de studiu	Nr. de ore
Tema 1. Introducere în securitatea informației		
1.	Obiectul de studiu al securității informațiilor.	2
2.	Atribute de securitate a informațiilor.	
3.	Amenințări la adresa securității informației.	
Tema 2. Aspecte juridice privind protecția și securitatea informației		
1.	Noțiuni generale ale aspectului legislativ de protecție a informației.	2
2.	Infrațiuni informatice și infrațiuni în domeniul telecomunicațiilor.	
3.	Secretul de stat și secretul comercial.	
4.	Alte acte legislative conexe securității informaționale.	
5.	Concepția securității informaționale a Republicii Moldova.	
Tema 3. Standarde în domeniul securității informației		
1.	Introducere în standardizare.	2
2.	Evoluția standardelor de securitate.	
3.	Familia de standarde ISO/IEC 27000	
Tema 4. Aspectul organizatoric de asigurare a securității informaționale		
1.	Măsuri administrative de protecție a informației.	2
2.	Măsuri procedurale de protecție a informației.	
Tema 5. Vulnerabilități și amenințări la adresa securității informației		
1.	Noțiunea de amenințare la adresa securității informației.	2
2.	Software-ul rău intenționat.	
3.	Tipuri de atacuri informatice.	
4.	Vulnerabilități de securitate.	
Tema 6. Metode și mijloace tehnice de protecție a informației		
1.	Identificarea și autentificare.	2
2.	Controlul accesului.	
3.	Responsabilitatea și auditul.	
4.	Protecția sistemelor și a comunicațiilor.	
Tema 7. Securitatea rețelelor de calculatoare		
1.	Noțiunea de securitate a rețelei.	2
2.	Atacuri asupra rețelelor de calculatoare.	
3.	Noțiune de atac pasiv și atac activ.	
4.	Atacul Denial of Service. Atacurile bazate pe browser.	
5.	Atacurile de tip brute-force. Atacurile asupra SSL.	
6.	Scanarea porturilor. Atacuri DNS. Atacurile backdoor.	
7.	Atacurile Shellshock. Atacuri de tip Botnet.	
Tema 8. Sisteme de detectare și prevenire a intruziunilor (Intrusion Detection System - IDS)		
		2

Nr. d/o	Subiectele de studiu	Nr. de ore
1.	Noțiunea de IDS. Arhitectura IDS.	
2.	Avantaje și dezavantaje ale IDS.	
3.	Metode de identificare a traficului rău-intenționat.	
4.	Sisteme de prevenire a intruziunilor.	
5.	Software-ul antivirus (anti-malware).	
6.	Sisteme de prevenire a scurgerilor/pierderilor de date.	
7.	Rețele virtuale private.	
Tema 9. Firewall-ul		2
1.	Noțiune de Firewall. Firewall NGFW de nouă generație.	
2.	Tipurile de Firewall. Rolul unui paravan de protecție.	
3.	Monitorizarea și inspectarea traficului prin Firewall.	
4.	Aplicarea unor reguli Firewall pentru restricționarea conexiunilor .	
5.	Supravegherea sistemelor Firewall pe Internet. Tehnici de filtrare a traficului.	
6.	Modul de funcționare. Politica paravanelor de protecție.	
7.	Importanța paravanului de protecție pe Internet.	
Tema 10. Protocoale de securitate în rețea		2
1.	Protocoale la Nivelul Aplicație.	
2.	Protocoale la Nivelul Transport.	
3.	Protocoale la Nivelul Rețea.	
4.	Protocoale la Nivelul Legătură de Date.	
Tema 11. Phishing - metodă de furt de identitate		2
1.	Noțiunea de Phishing. Phishing-ul prin intermediul e-mail-ului, telefonului.	
2.	Funcționarea Phishing-ului. Tipurile de atacuri Phishing.	
3.	Protejarea de excrocherii prin Phishing.	
4.	Evaluarea cursului teoretic	2
Total		24

Laborator (16 de ore)

Nr. d/o	Tematica lecțiilor de laborator	Nr. de ore
1.	Tehnici de atac asupra aplicațiilor Web.	2
2.	Filtrarea datelor. Vulnerabilitățile SQL si LDAP Injection.	2
3.	Filtrarea datelor. Vulnerabilitatea XSS. Filtrarea datelor. Null byte injection.	2
4.	Filtrarea datelor. File injection.	2
5.	Autorizarea si autentificarea. Criptarea parolelor.	2
6.	Autorizarea si autentificarea. Brut force. Vulnerabilitatea CSRF.	2
7.	Tehnica de atac DDoS. Tehnica de atac Fingerprinting.	2
8.	Scanarea serverului. Fișierul htaccess. Configurarea Firewall.	2
Total		16

Strategii didactice utilizate

În cadrul unității de curs *Gestiunea securității informatice* se aplică următoarele metode de predare și de învățare: expunerea, prelegerea interactivă, lucrări de laborator, conversația, demonstrația didactică (metoda vizuală), problematizarea, explicarea (prin intermediul atât a instrumentului interactiv, didactic și profesional – tabla interactivă, cât și prin intermediul unui procesor de prezentări) etc. De asemenea, pe parcursul studierii unității de curs se vor utiliza strategii didactice centrate pe student: instruire diferențiată, tehnici de dezvoltare a gândirii critice, instruirea prin problematizare și instruirea prin proiecte.

Pentru asigurarea realizării strategiilor didactice menționate se vor utiliza suportul de curs, culegere de prezentări de sinteză PowerPoint, consultații individuale.

Activități de lucru individual

Rezultatele activității individuale ale studenților sunt incluse într-un portofoliu personal al fiecărui student și sunt prezentate public la finele cursului respectiv. Sarcinile pentru lucrul individual, cerințele și indicațiile de realizare a acestora sunt înaintate de către cadrul didactic la orele de laborator.

Evaluarea

Evaluarea studenților la unitatea de curs *Gestiunea securității informatice*, se realizează în corespundere cu Regulamentul de organizare a studiilor superioare de masterat (Ciclul II) în Universitatea de Stat „Alec Russo” din Bălți și cu Regulamentul-cadru privind evaluarea cunoștințelor studenților, obținute în procesul de formare și a rezultatelor academice ale studenților în Universitatea de Stat „Alec Russo” din Bălți.

Cunoștințele, capacitățile și competențele studenților obținute pe parcursul studierii cursului respectiv vor fi apreciate printr-o evaluare curentă la finele cursului teoretic; o evaluare curentă în afara orelor de contact direct, din contul orelor de studiu individual; realizarea sarcinilor de lucru individual; realizarea lucrărilor de laborator.

Nota semestrială va reprezenta media aritmetică a tuturor notelor acumulate la orele de curs, laborator și la lucrul individual.

Nota finală (N_f) la unitatea de curs se calculează conform formulei: $N_f = N_s \times 0.5 + N_{ex} \times 0.5$, unde N_s – nota semestrială, N_{ex} – nota de la examen.

Evaluarea finală are loc sub forma unui test ce include întrebări atât din cursul teoretic, cât și practic. Timpul rezervat pentru rezolvarea testului este de 80 de minute.

La finalizarea cursului, studentul evaluează prin completarea anonimă a unui chestionar în variantă electronică atât unitatea de curs respectivă, cât și cadrele didactice implicate, în scopul îmbunătățirii procesului de instruire la unitatea de curs respectivă.

Bibliografie

1. ANDERSON, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Ed. „Wiley”, 2008, ISBN-13: 978-0470068526;
2. BISHOP M., *Computer Security: Art and Science*, Addison-Wesley, 2003.
3. CAMPBELL T. *Practical Information Security Management: A Complete Guide to Planning and Implementation*, Apress, 2016.
4. KAUFMAN C., PERLMAN R., SPECINER M. *Network Security: Private Communication in a Public World*, Second Edition Prentice Hall PTR 2002.
5. KELLY L., MCCUMBER J. *Assessing and Managing Security Risk in IT Systems*, CRC Press, 2005.
6. TANENBAUM, A. *Rețele de calculatoare* - Ed. a 4-a. București, Editura „Bucuresti”, 2008, ISBN: 973-97706-3-0.
7. TIPTON H., KRAUSE M. *Information Security Management Handbook - Fifth Edition*, CRC Press, 2004.
8. ZGUREANU, A. *Bazele securității informației*. Centrul Editorial-Poligrafic al ASEM. Chișinău, 2018. – 242 p. ISBN 978-9975-75-912-0.
9. ПАНАСЕНКО, С. *Алгоритмы шифрования. Специальный справочник*. Санкт-Петербург, Издательство „БХВ - Петербург”, 2009, ISBN: 978-5-9775-0319-8. Sommerville I. *Software Engineering*, Addison Wesley, Boston, 2001, 773 p.
10. ШАНЬГИН, В., *Информационная безопасность компьютерных систем и сетей*. Москва, Издательство „Форум”, 2008, ISBN: 978-5-8199-0331-5.
11. ШНАЙДЕР, Б. *Секреты и лож. Безопасность данных в цифровом мире*. Санкт-Петербург, Издательство „Питер”, 2008, ISBN: 5-318-00193-9.

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 salutăată poziția activă a studentului care studiază din propria inițiativă noi conținuturi, propune soluții (aplicații, instrumente Web etc.), formulează întrebări în cadrul prelegerilor și a orelor de laborator.
3. În cadrul unității de curs 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, el este obligat să efectueze toate lucrările de laborator la care a lipsit și să le susțină conform orarului consultațiilor curente la unitatea de curs, 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 „Alec Russo” din Bălți.
6. Nu este salutăată întârzierea la ore.