

UNIVERSITATEA DE STAT DIN MOLDOVA
FACULTATEA RELATII INTERNATIONALE, STIINTE POLITICE SI
ADMINISTRATIVE
DEPARTAMENTUL RELATII INTERNATIONALE

CURRICULUM

la unitatea de curs/modulul

„Securitatea informatională”

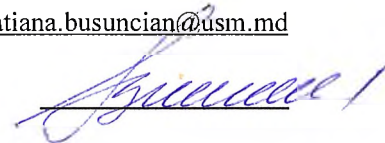
Ciclul II, Specialitatea Studii Diplomatice

AUTOR:

Tatiana BUSUNCIAN,

Dr., conf. univ.

tatiana.busuncian@usm.md



APROBAT

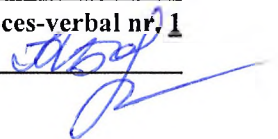
la ședința Departamentului

din „28” august 2025

proces-verbal nr. 1

Sef Departament





APROBAT

la ședința Consiliului Facultății

din „28” august 2025

proces-verbal nr. 1

Decan



CHIȘINĂU 2025

PRELIMINARII

Prezentarea generală a disciplinei „Securitatea Informațională”. Disciplina Securitate informațională prezintă prin tematica și obiectivele trasate un studiu conceptual-teoretic și cu valențe aplicative, orientat spre asigurarea cunoașterii, înțelegerii și explicării de către masteranzi a principalelor noțiuni, sintagme și abordări privind relațiile internaționale tratate ca sistem, concepte, categorii și strategii ale securității informaționale contemporane.

Locul și rolul disciplinei Securitatea informațională în formarea rezultatelor învățării ale specialității Relații internaționale și misiunea curriculumului în formarea profesională.

Disciplina Securitatea Informațională este un curs teoretico-metodologic și științifico-aplicativ deosebit de important pentru aprofundarea familiarizării masteranzilor cu cerințele de cercetare științifică în domeniul relațiilor internaționale, în vederea realizării studiilor teoretico-analitice, inclusiv a tezelor de master. Disciplina vine să caracterizeze evoluarea problemelor actuale în domeniul de securitate a informațiilor prin prisma artei diplomatice, a relațiilor optime de colaborare, a procedurilor și metodelor acestora pentru a familiariza masteranzii despre rolul și importanța securității informaționale în realizarea politicii interne și externe a statelor. Programul presupune o incursiune profundă în noțiunile conexe și concurente privind dimensiunea structural-funcțională a securității informaționale în noul context de securitate din perspectiva eficacității formelor colaborării internaționale, inclusiv a organelor securității statului din Republica Moldova. Studiarea acestei discipline va contribui la formarea și dezvoltarea de competențe profesionale.

Limba de predare a disciplinei este limba română.

Beneficiarii disciplinei „Securitatea Informațională” este destinat masteranzilor Ciclului I, studii integrate, anul 1, fiind elaborat în corespundere cu prevederile planului de studii, axându-se pe formarea la masteranzi a cunoștințelor la nivel de cunoaștere, aplicare și integrare, orientați spre politici, care subliniază și îi învață pe specialiștii din domeniul securității, diplomației, relațiilor internaționale cum să ia decizii în cunoștință de cauză în materie de politică de securitate, strategie și planificare în cadrul cooperării și al abordărilor în sectoarele public și privat. Programul îi ajută pe participanți să aprecieze natura și amploarea amenințărilor de astăzi și dezvoltă o înțelegere comună a lexicului, a celor mai bune practici și a inițiativelor informaționale actuale în sectoarele public și privat. Formarea în acest domeniu este crucială pentru consolidarea securității la nivel național și internațional, gestionarea eficientă a provocărilor și riscurilor de securitate.

I. ADMINISTRAREA DISCIPLINEI

Forma de învățământ	Codul unității de curs/modulului	Denumirea unității de curs/modulului	Responsabil de unitatea de curs/modulul	Semestrul	Ore							Evaluarea	Nr. de Credite
					Total	Contact direct			FPPU *	Studiu individual			
						C	S	L		asin cron*	indiv dual		
cu frecvență	S.A.10	Securitatea Informațională	Busuncian Tatiana	II	180	15	30	135				Ex.	6
cu frecvență redusă													
la distanță													
cu frecvență dual													

*formare profesională practică la unitate - pentru învățământul dual

*pentru învățământul cu frecvență redusă și la distanță

II. TEMATICA ȘI REPARTIZAREA ORIENTATIVĂ A ORELOR

N r. d/ o	Unități de conținut	Ore															
		Curs				Seminar				FPPU	Studiu individual						
		Cu frecvență	f/r	La distanță	dual	Cu frecvență	f/r	La distanță	dual		dual	Cu frecvență	f/r		La distanță		dual
asincron	individual									asincron			individual				
1.	Istoriografia cercetării securității informaționale	2				2					14						
2.	Securitatea informațională: concepte și noțiuni	2				2					14						
3.	Protecția informației. Prevenirea și curmarea fraudelor informatice	2				6					20						
4.	Dezvoltarea cooperării internaționale în domeniul securității informaționale	2				4					16						
5.	Războiul informațional: tendințe, amenințări, perspective	2				4					18						
6.	Securitatea informațională și activitatea serviciilor de informații în contextul globalizării	2				4					18						
7.	Securitatea informațională și terorismul – preocupare globală	1				4					17						
8.	Islamul radical. Mecanisme de recrutare în mediul online.	2				4					18						
Total		15				30					135						

III. COMPETENȚE GENERALE, PROFESIONALE ȘI REZULTATELE ÎNVĂȚĂRII

COMPETENȚE GENERALE (CG)	REZULTATELE ÎNVĂȚĂRII (RI) <i>Absolventul/candidatul la atribuirea calificării poate</i>
CG 1. Argumentarea fenomenelor și proceselor din domeniul securității informaționale la nivel național și internațional, în baza gestionării eficiente a informației în contextul securității.	RI 2 a evalua și argumenta situațiile și procesele din domeniul securității informaționale la nivel național și internațional, pe baza colectării, verificării și gestionării eficiente a informațiilor.
CG 4. Dimensiunea securității și gestionării informațiilor în procesele strategice.	RI 6 a utiliza tehnici și instrumente de management strategic pentru planificarea și gestionarea securității informaționale în cadrul organizațiilor și instituțiilor politice.
CG 5. Asigurarea comunicării și cooperării instituționale în domeniul securității informaționale.	RI 9 a facilita comunicarea și cooperarea instituțională pentru coordonarea activităților și schimbului de informații în domeniul securității informaționale.
COMPETENȚE PROFESIONALE (CP)	REZULTATELE ÎNVĂȚĂRII (RI)
CP 2. Implementarea strategiilor în gestionarea conflictelor și crizelor internaționale.	RI 13 analiza și elabora strategii de gestionare a conflictelor și crizelor internaționale, prin aplicarea principiilor și mecanismelor de securitate informațională.
CP 6. Expertiza problemelor și tendințelor din domeniul relațiilor internaționale, elaborarea de politici în domeniul securității informaționale în context internațional.	RI 17 dezvoltă propuneri de proiecte și politici în domeniul relațiilor internaționale, integrând analiza riscurilor și provocărilor de securitate informațională.
CP 7. Consiliere în realizarea și reflectarea capacității de analiză, evaluare și elaborare de materiale analitice relevante pentru securitatea informațională.	RI 18 realiza studii, evaluări și rapoarte analitice, precum și scenarii de evoluție a situațiilor de securitate internațională, pentru fundamentarea deciziilor în domeniul politicii externe.

Notă. Competențele și rezultatele învățării vor fi însoțite de cod și număr de ordine conform Standardului de calificare.

IV. UNITĂȚI DE ÎNVĂȚARE

Tema 1. ISTORIOGRAFIA CERCETĂRII SECURITĂȚII INFORMAȚIONALE		
Rezultatele învățării preconizate a fi atinse: RI 2; RI 6; RI 18		
Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>securitate informațională; securitatea informației, securitate cibernetică, noțiuni, instrumente, stat.</i> Unități de conținut: 1. Istoriografia cercetării securității informaționale, obiectul de studiu, structura cursului, sursele bibliografice pe domeniul securității informaționale; 2. Locul cursului printre alte discipline din domeniul programului "Studii de securitate și Managementul Informației", importanța teoretică și practică a studiului; 3. Noțiunea de "securitate informațională", instrumente și metode de lucru, rolul securității informaționale în realizarea securității naționale a statului.	- Relatează despre istoriografia cercetării securității informaționale; - Dezvoltă obiectul de studiu și structura cursului; - Proiectează locul și rolul cursului printre alte discipline din domeniul programului "Studii de securitate și Managementul Informației", importanța teoretică și practică al programului; - Definește noțiunea de "securitate informațională"; - Evaluează rolul securității informaționale, importantă resursă pentru organizații responsabile de luarea deciziilor.	Masterandul manifestă o implicare responsabilă și autonomă în elaborarea metodologiei de cercetare în domeniul istoriografiei securității informaționale, inclusiv în școlile și curentele istoriografice de cercetare care explorează locul și rolul dimensiunii informaționale în studiile de securitate.
Tema 2. SECURITATEA INFORMAȚIONALĂ: CONCEPTE ȘI NOȚIUNI		
Rezultatele învățării preconizate a fi atinse: RI 2; RI 6; RI 18		
Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>securitate informațională, concepte, noțiuni, riscuri, crime, fraude, război informațional, stat, etc.</i> Unități de conținut: 1. Concepte și noțiuni privind securitatea informațională; 2. Evoluția și accesul la tehnologia informației - un număr tot mai mare de incidente cibernetice motivate politic împotriva securității statelor; 3. Instrumente și metode de lucru pentru îmbunătățirea strategiilor de securitate națională/internațională.	- Distinge principalele concepte și noțiuni de securitate informațională, argumentează importanța și necesitatea unei strategii care să cuprindă reglementări comprehensive ale tuturor vectorilor securității informaționale; - Determină rolul statului în gestionarea problemelor de securitate informațională; - Estimează riscurile, crimele și fraudele informaționale; - Evaluează politica de securitate a	Masterandul se implică responsabil și autonom în analiza multiplelor surse pentru a analiza și formula concluzii bine fundamentate și pentru a oferi perspective solide asupra evoluțiilor de securitate informațională, identifică potențialele amenințări și vulnerabilități în contextul securității naționale și internaționale, elaborează scenarii și dezvoltă studii prospective, analizând tendințele actuale și viitoare.

	informației în cadrul instituțiilor publice și metodologia cercetării.	
Tema 3. PROTECȚIA INFORMAȚIEI. PREVENIREA ȘI CURMAREA FRAUDELOR INFORMATICE		
Rezultatele învățării preconizate a fi atinse: RI 6; RI 13; RI 17		
Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>securitate informațională, atacuri de tip malware, atacuri de tip phishing, atacuri de tip DDoS, atacuri asupra infrastructurii critice, atacuri de manipulare a informațiilor, securitatea cibernetică, riscurile cibernetică, măsuri tehnice de securitate cibernetică, actualizarea i patch-urile software, backup-uri și planuri de recuperare în caz de dezastru.</i> Unități de conținut: - Protecția informațiilor sensibile și infrastructurii critice, asigurarea securității informaționale; - Procesul de comunicare strategică între sectorul de securitate al Republicii Moldova, mediului științific și societatea civilă; - Elucidarea aspectelor combaterii știrilor false și identificarea eficientă a căilor de soluționare a acestora în condițiile provocărilor de securitate.	- Definește caracteristicile securității informaționale; - Determină instrumentele și metodele de luptă cu amenințările cibernetice; - Evaluează motivele criminalității cibernetice și descrie eforturile întreprinse pentru asigurarea securității informaționale și de securitate națională, în general; - Estimează importanța prevenirii amenințărilor complexe și persistente la adresa securității informaționale.	Absolventul în mod autonom poate aplica reguli de bază pentru protejarea informațiilor personale și sensibile în mediul online; utilizează instrumente și metode de prevenire și estimare a amenințărilor complexe la adresa securității informaționale.
Tema 4: DEZVOLTAREA COOPERĂRII INTERNAȚIONALE ÎN DOMENIUL SECURITĂȚII INFORMAȚIONALE		
Rezultatele învățării preconizate a fi atinse: RI 9; RI 13; RI 17		
Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>colaborare, securitate informațională, programe internaționale, acorduri, negocieri.</i> Unități de conținut: Căile de colaborare a instituțiilor responsabile de securitatea informațională în	Identifică căile de colaborare internațională a instituțiilor responsabile de securitatea informațională în domeniul prevenirii și combaterii terorismului și criminalității transfrontaliere;	Masterandul demonstrează o implicare autonomă în promovarea și consolidarea valorilor democratice, prin dobândirea unei înțelegeri profunde despre colaborarea internațională și regională în

domeniul prevenirii și combaterii terorismului și criminalității transfrontaliere; 2. Inițierea negocierilor privind semnarea acordurilor de cooperare la nivel internațional pentru îmbunătățirea capacității de răspuns în cazul unor atacuri cibernetice majore; 3. Interesele naționale de securitate informațională în formatele de cooperare internațională la care Republica Moldova este parte.	- Analizează principalele direcții de colaborare în acest domeniu, inițiază negocieri privind semnarea acordurilor de cooperare la nivel internațional pentru îmbunătățirea capacității de răspuns în cazul unor atacuri cibernetice majore; - Determină interesele naționale de securitate informațională în formatele de cooperare internațională la care Republica Moldova este parte;	domeniul securității informaționale în contextul noilor amenințări emergente, propune soluții pentru îmbunătățirea colaborării internaționale în cazuri de amenințări cibernetice globale.
---	--	--

Tema 5: RĂZBOIUL INFORMAȚIONAL: TENDINȚE, AMENINȚĂRI, PERSPECTIVE

Rezultatele învățării preconizate a fi atinse: RI 2; RI 6; RI 13

Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>securitate informațională, război informațional, mediu informațional, pericol, politică.</i> Unități de conținut: - Istoriografia cercetării războiului informațional, geneza și trăsăturile războiului informațional; - Forme de manifestare pe arena internațională, practici și strategii ale actorilor internaționali împotriva războiului informațional și procesul de asigurare a securității naționale și internaționale; - Impactul războiului informațional asupra securității naționale a Republicii Moldova, practici și instrumente de luptă a Republicii Moldova împotriva războiului informațional.	- Identifică geneza și trăsăturile războiului informațional; - Determină forme de manifestare pe arena internațională; - Evaluează practici și strategii ale actorilor internaționali împotriva războiului informațional și în procesul de asigurare a securității naționale și internaționale; - Analizează impactul războiului informațional asupra securității naționale a Republicii Moldova; - Estimează practici și instrumente de luptă a Republicii Moldova împotriva războiului informațional.	Absolventul în mod autonom poate identifica metodele de propagandă și manipulare în formatică în spațiul online; evalua impactul războiului informațional asupra opiniei publice și a relațiilor internaționale; dezvolta strategii de reziliență la nivel individual și societal împotriva manipulării informaționale (educație, media, gândire critică).

Tema 6. SECURITATEA INFORMAȚIONALĂ ȘI ROLUL SERVICIILOR DE INFORMAȚII ÎN CONTEXTUL NOILOR AMENINȚĂRI INFORMAȚIONALE GLOBALE

Rezultatele învățării preconizate a fi atinse: R2 1; RI 9; RI 17

Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>Sectorul de securitate, reziliență, riscuri, amenințări, vulnerabilități de securitate, capacitate de reziliență și</i>	- Identifică activitatea serviciilor de informații în contextul noilor amenințări informaționale globale;	Masterandul poate în mod autonom gestiona și analiza scenarii de conflict, utilizând trinomial vulnerabilitate-risc-

<i>răspuns, cultura de securitate, riscurile cibernetice, măsuri tehnice de securitate cibernetică, actualizarea și patch-urile software, backup-uri și planuri de recuperare în caz de dezastru.</i> Unități de conținut: 1. Activitatea serviciilor de informații în contextul amenințărilor hibride, adaptarea acestora la noile riscuri și amenințări la adresa securității informaționale; 2. Cooperare pe arena internațională în domeniul securității informaționale a serviciilor/agențiilor/comunităților de informații; 3. Conlucrarea serviciilor de informații în dezvoltarea colaborării eficiente privind creșterea transparenței instituționale.	- Relatează despre adaptarea serviciilor de informații la noile riscuri și amenințări la adresa securității informaționale; - Analizează cadrul de cooperare pe arena internațională în domeniul securității informaționale a serviciilor/agențiilor/comunităților de informații; - Elaborează noi responsabilități pe conlucrarea a serviciilor de informații ce țin de dezvoltarea unei colaborări eficiente privind creșterea transparenței instituționale.	amenințare și de a corela problemele fundamentale și fenomenele asociate cu riscurile, vulnerabilitățile și amenințările la adresa securității; evalua protecția datelor sensibile, ținând cont de respectarea legislației și transparența față de public; formulează decizii, supraveghează și controlează respectarea legilor și a drepturilor individuale în domeniul securității informaționale.
--	--	---

Tema 7. SECURITATEA INFORMAȚIONALĂ ȘI TERORISMUL – PREOCUPARE GLOBALĂ

Rezultatele învățării preconizate a fi atinse: RI 2; RI 6; RI 13

Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>securitate informațională, terorism internațional, terorism religios, terorism etnic, terorism politic, terorism ideologic, terorism de stat, grupuri teroriste, motivații teroriste, metode teroriste, atacuri teroriste, radicalizare, extremism violent, rețele teroriste, propagandă teroristă, recrutare teroristă, contraterorism, prevenirea terorismului, măsuri de securitate, inteligență și supraveghere, victime ale terorismului, legislație antiteroristă, justiție penală.</i> Unități de conținut: 1. Istoriografia cercetării securității informaționale, noțiunea de securitate informațională și terorism;	- Relatează despre istoriografia cercetării securității informaționale; - Definește noțiunea de securitate informațională, noțiunea de terorism; - Estimează provocările actuale în domeniul securității informaționale; - Evaluează eficiența și rolul colaborării internaționale a serviciilor de informații în domeniul prevenirii și combaterii terorismului.	Absolventul în mod autonom și responsabil poate elabora metodologii de cercetare în domeniul securității informaționale și a terorismului, inclusiv defini noțiunea de securitate informațională, noțiunea de terorism; estima provocările actuale și evalua eficiența și rolul colaborării internaționale a serviciilor de informații în domeniul prevenirii și combaterii terorismului.

2. Provocările actuale în domeniul securității informaționale; 3. Colaborarea internațională a serviciilor de informații în domeniul prevenirii și combaterii terorismului.		
Tema 8. ISLAMUL RADICAL. MECANISME DE RECRUTARE ÎN MEDIUL ONLINE		
Rezultatele învățării preconizate a fi atinse: RI 6; RI 13; RI 18		
Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>radicalizare, spațiul virtual, atac cibernetic riscuri, amenințări, vulnerabilități de securitate, capacitate de reziliență și răspuns, organizații europene și internaționale specializate, contracararea terorismului, strategii antiteroriste, măsuri de securitate, legislație antiteroristă, operațiuni antiteroriste, prevenirea terorismului, contrapropagandă, reabilitare și reintegrare, controlul armamentului, amenințări emergente.</i> Unități de conținut: - Instrumente și mecanisme de prevenire a radicalizării și oclotirii valorilor, garantării securității cetățenilor în spațiul virtual. - Evaluarea și determinarea metodelor de radicalizare a islamiștilor prin intermediul rețelelor. - Scopuri teroriste online prin intermediul propagandei și radicalizării care conduc la terorism în mediul online.	- Identifică instrumentele și mecanismele de prevenire a radicalizării și oclotirii valorilor, garantării securității cetățenilor în spațiul virtual; - Evaluează și determină metodele de radicalizare a islamiștilor prin intermediul rețelelor; - Analizează scopurile teroriste online prin intermediul propagandei și radicalizării care conduc la terorism în mediul online.	Absolventul în mod autonom și responsabil poate aplica instrumente și mecanisme de prevenire a radicalizării în spațiul virtual; utilizează metode de prevenire și estimare a amenințărilor la adresa securității informaționale; analizează și identifică contextul extremist respectând drepturile fundamentale și libertățile civile.

Notă. **Responsabilitate și autonomie** exprimă un comportament format (într-o formulare generalizată) ca rezultat în cadrul respectivei unități de învățare.

V. STUDIUL INDIVIDUAL AL STUDENTULUI

Nr.	Produsul preconizat	Strategii de realizare	Criterii de evaluare	Termen de realizare
1.	Proiect de cercetare: Impactul dezinformării online asupra securității naționale și relațiilor internaționale	Strategii de realizare: - Determinarea actualității și importanței problemei abordate, a scopului, obiectivelor, cuvintelor cheie - Descrierea conceptelor și noțiunilor de securitate informațională și elementele sale componente - Identificarea obiectivelor principale de referință ale securității informaționale - Abordarea teoretico-metodologică a conceptului de "securitate informațională" - Analiza riscurilor și amenințărilor potențiale la adresa securității informaționale și semnificației acestora în relațiile politice, economice și comerciale - Evaluarea tendințelor, amenințărilor și perspectivelor războiului informațional - Definirea și tipologia conflictelor internaționale, fazele conflictului. - Estimarea pericolului terorismului internațional, situație care poate pune în primejdie existența întregii omeniri (exemple) - Proiectarea argumentelor cu privire la strategii globale de asigurare a securității informaționale - Elaborarea concluziilor și recomandărilor. - Identificarea dimensiunii ontologice și epistemologice al Relațiilor internaționale, conceptelor și noțiunilor, securitate informațională și politică externă, mișcările teroriste și alți actori nestatali, fenomenele globalizării și regionalizării. - Evaluarea legăturii dintre	Față de cercetare: - Prezentarea produsului în termenele stabilite - Gradul corespunderii temei cu esența materialului cercetării - Identificarea și justificarea relevanței și profunzimii studiului - Parcurgerea și interacțiunea cu o bibliografie, prezența referințelor de subsol - Structurarea materialului, analiza/prelucrarea datelor: elaborarea/definirea termenilor; furnizarea de explicații; indicarea relevanței explicațiilor - Identificarea posibilităților de aplicare a rezultatelor - Respectarea calitățile fundamentale ale stilului: concizie, claritate, proprietate; coerență; coeziune - Corespunderea conținutului rigorilor, respectarea cerințelor tehnice - Relevanța concluziilor Față de ppt: - Abordarea tridimensională: narativă, descriptivă și argumentativă - Claritatea: o structură bine conturată - Interacțiunea cu materialul bibliografic - Originalitate, creativitate, inovație, coerență logică - Corespunderea rigorilor: gramatica, ortografia, aspectul estetic - Relevanța concluziilor	Pe parcursul semestrului

		aspectele teoretice și cele practice ale relațiilor internaționale - Proiectarea noului sistem de securitate informațională. Modalități de prezentare: <i>În scris</i> – sub formă de cercetare în grup, în format Word, în volum de 20-25 pagini (text cules cu Times New roman, font 12, 1,5 între rânduri, spațiul – 3 cm, 2,5 cm, 2,5 cm, 1,5 cm; format electronic) și <i>verbal</i> – sub formă de PPT în cadrul unei mese rotunde		
2.	Dezbateri și analiza critica a transformărilor în securitatea informațională: Sesiuni de discuții pentru a încuraja schimbul de idei și perspective.	• Discuții pe marginea diverselor perspective și opinii asupra schimbărilor în securitatea informațională. • Evaluarea impactului transformărilor asupra mediului de securitate internațional.		<i>La sfârșitul semestrului</i>
3.	Simulări și studii de caz pentru aplicarea cunoștințelor teoretice. Dezbateri: Opțiuni de consolidare a sectorului securității naționale împotriva amenințărilor și conflictelor hibride Sesiuni de discuții pentru a încuraja schimbul de idei și perspective.	Abilitatea de a lucra în echipă și de a negocia cu diverse părți interesate pentru a promova soluții și politici de securitate eficiente și acceptabile.	Profunzimea studiului - Diversitatea surselor. - Analiza critică a rezultatelor prezentate. - Identificarea posibilităților de aplicare a rezultatelor. - Relevanța concluziilor. - Originalitatea formei de prezentare.	<i>Pe parcursul semestrului</i>

VI. SUGESTII METODOLOGICE DE PREDARE-ÎNVĂȚARE-EVALUARE

• Formele de organizare a instruirii:

Formele principale ale instruirii sunt cursul și seminarul. Cursul este organizat sub formă de prelegere clasică, dezbateri, poate fi curs mixt prelegere – dezbateri, curs practic – aplicativ, prelegere problematizată. Seminarul de asemenea are mai multe forme: seminare de reluare și aprofundare a anumitelor probleme abordate în cadrul cursului, de realizare a corelațiilor intra-inter și transdisciplinare; dezbateri, brainstorming, în baza cercetării, a studiului de caz. Metode de lucru: expunerea, explicația, dialogul, prezentarea, lucrul în grup, masă rotundă, metoda Piramidei, Jigsaw (Mozaicul), etc.

- **Strategii/ tehnologii didactice aplicate**

Tehnologiile și strategiile didactice aplicate în predare cursului se instituie atât în raport de implicație cât și de complementaritate funcțională. Astfel, strategiile și tehnologiile didactice aplicate sunt expunerea didactică, conversația didactică, demonstrația, lucrul cu actele normative, modelarea didactică, problematizarea. În cadrul cursului se organizează simulări ale medierii /negocierii unor conflicte posibile în activitatea administrativă, diferite activități frontale, activități de grup, activități individuale.

- **Strategii de evaluare a rezultatelor academice, inclusiv cu indicarea modalității de calcul a notei finale.**

Evaluarea curriculară se aplică prin trei forme: inițială, intermediară și finală.

1. Evaluarea inițială/diagnostică, orală se efectuează la începutul activităților de predare pentru a stabili gradul de pregătire a masteranzilor pentru cursul preconizat, potențialul de învățare la începutul unei noi activități. Se apreciază prin *interviu, chestionare orală, conversație, expuneri orale*, cunoștințele, abilitățile și competențele profesionale formate pe parcursul ciclului I, pentru a ști dacă sunt apti să se integreze cu șanse de reușită în noul program de instruire, pentru realizarea noilor obiective.

2. Evaluarea continuă/dinamică formativă, scrisă se efectuează sub forma a *două lucrări de control* petrecute în cadrul orelor practice, pe un grup de teme cu subiecte ce cuprind cele trei nivele (cunoaștere, aplicare, integrare), și *lucrări de laborator*, cu scopul de a cunoaște dacă și în ce măsură obiectivele privind cunoștințele și capacitățile ce trebuiau însușite au fost atinse. Demersul vizează atât cunoașterea progreselor masterandului, cât și identificarea dificultăților de învățare pe care le întâmpină. Pornind de la esența evaluării dinamice, constatăm caracterul formativ al acesteia.

La stabilirea notei finale se iau în considerare		
- testarea continuă pe parcursul semestrului, rezultatele activității la seminare / lucrări practice de laborator	cel puțin 60%	20%
- testarea periodică prin lucrări de control		10%
- activitățile individuale teme / referate / eseuri / traduceri / proiecte, studiu de caz, etc.		30%
- activități practice		0%
- alte activități (precizați)		0%
rezultatele de la examenul final	cel mult 40%	40%

BIBLIOGRAFIE RECOMANDATĂ:

Pe suport de hârtie

1. Busuncian T. Information resilience of the Republic of Moldova in the context of emerging hybrid threats. Conferință, manifestare științifică internațională: Universitas Europaea: spre o societate a cunoașterii prin europenizare și globalizare. 16-17 octombrie 2025, pp. 488-493.
https://conferinte.stiu.md/sites/default/files/evenimente/Volum_Conferinta_ULIM_16-17.X.2025.pdf
2. Busuncian T., Moldovan I. Importanța asigurării securității cibernetice în cadrul domeniului politic: probleme, riscuri și noi oportunități. Materialele conferinței: Securitatea națională a Republicii Moldova: provocări și tendințe. INIS, Chișinău 14 mai 2022, pp. 101-110.
3. Busuncian T. Securitatea informațională și activitatea serviciilor de informații în contextul globalizării. Studii naționale de securitate. Revistă științifico-practică Nr. 1 (1) 2020. ISSN 2587-3822 CZU 004.056: 355.40 DOI: 10.5281/zenodo.3989164. Chișinău, 2020, p. 66-78.
4. Busuncian T. Parametrii instituționali ai securității informaționale. Materialele conferinței științifico-practice naționale „Mandatul de securitate: probleme actuale de interpretare, legislație și practică”. Serviciul de Informații și Securitate al Republicii Moldova Institutul Național de Informații și Securitate „Bogdan, Întemeietorul Moldovei”. Chișinău, 2020, p. 71-75.
5. Busuncian T. Pericolul știrilor false asupra securității informaționale. Materialele mesei rotunde. Combaterea știrilor false în condițiile provocărilor de Securitate. INIS, Chișinău 2020. ISBN 978-9975-3271-0-7. 20 mai 2020, p. 27-35.
6. Busuncian T. Radical Islam. Recruitment Mechanisms in Immediate Neighborhood with European Union. In: Eastern Europe - Regional Studies, 2020, number 1. ISSN: 2587-456X
<http://www.psage.tsu.ge/index.php/Easternstudies/article/view/186/0>
7. Busuncian T. Istoriografia, bazele teoretico-conceptuale și metodologice ale cercetării teoriei și practicii securității informaționale și colaborării internaționale a serviciilor speciale. În: Relațiile internaționale în curriculumul universitar: bazele teoretico-metodologice. Coord. V. Teosa. Chișinău, 2016. ISBN 978-9975-70-899, pp. 245-260.

Surse electronice:

1. 2026 Global Digital Trust Insights Survey.
https://conferinte.stiu.md/sites/default/files/evenimente/Volum_Conferinta_ULIM_16-17.X.2025.pdf
2. State of Cybersecurity Rezilience 2025.
https://conferinte.stiu.md/sites/default/files/evenimente/Volum_Conferinta_ULIM_16-17.X.2025.pdf
3. Global Cybersecuurity Outlook 2026. Insight report, January 2026.
https://conferinte.stiu.md/sites/default/files/evenimente/Volum_Conferinta_ULIM_16-17.X.2025.pdf
4. Hibberd G. The Art of Cyber Security: A Practical Guide to Winning the War on Cyber Crime, 2022; 1st ed.
https://soeg.kb.dk/discovery/fulldisplay?docid=alma99124177146905763&context=L&vid=45KBDK_KGL:KGL&lang=en&search_scope=MyInst_and_CI&adaptor=Local%20Search%20Engine&tab=Everything&query=any,contains,Cyber%20security&offset=10
5. Hotărârea Nr. 55 din 17. 03. 2020 privind declararea stării de urgență, Publicat: Monitorul Oficial al Republicii Moldova Nr. 86 din 17. 03. 2020.
https://www.legis.md/cautare/getResults?doc_id=120817&lang=ro
6. Războiul electronic și inteligența artificială, 2024.
https://www.researchgate.net/publication/377248415_Razboiul_electronic_si_inteligența_artificială