

UNIVERSITATEA DE STAT DIN MOLDOVA

FACULTATEA RELAȚII INTERNAȚIONALE, ȘTIINȚE POLITICE ȘI ADMINISTRATIVE

DEPARTAMENTUL ȘTIINȚE POLITICE ȘI ADMINISTRATIVE

CURRICULUM

la disciplina

„Securitatea Informațională”

Ciclul II, MASTERAT

Programul „Studii de Securitate Națională”

AUTOR:

BUSUNCIAN Tatiana
dr., conf. universitar
busuncian@gmail.com

APROBAT

la ședința Departamentului
din „___” _____ 2025
proces-verbal nr. _____

Șef Departament _____

APROBAT

la ședința Consiliului Facultății
din „___” _____ 2025
proces-verbal nr. _____

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 II, Programul „Studii de Securitate Națională”, anul II, 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.03.A.17	Securitatea Informațională	Busuncian Tatiana	I	150	20	20	110			Ex.	5	
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					12						
2.	Securitatea informațională: concepte și noțiuni	2				2					12						
3.	Protecția informației. Prevenirea și curmarea fraudelor informatice	2				2					10						
4.	Dezvoltarea cooperării internaționale în domeniul securității informaționale	2				2					12						
5.	Războiul informațional: tendințe, amenințări, perspective	2				2					10						
6.	Securitatea informațională și activitatea serviciilor de informații în contextul globalizării	2				2					10						
7.	Securitatea informațională și terorismul – preocupare globală	2				2					12						
8.	Islamul radical. Mecanisme de recrutare în mediul online.	2				2					10						
9.	Securitatea informațională la nivel european	2				2					10						
10.	Pericolul știrilor false asupra securității informaționale	2				2					12						
Total		20				20					110						

III. COMPETENȚE GENERALE, PROFESIONALE ȘI REZULTATELE ÎNVĂȚĂRII

COMPETENȚE GENERALE (CG)	REZULTATELE ÎNVĂȚĂRII (RI) <i>Absolventul/candidatul la atribuirea calificării poate</i>
CG 1. Argumentarea și evaluarea riscurilor și amenințărilor la adresa securității informaționale	RÎ1. interpreta datele referitoare la incidentele de securitate informațională, identificând tendințele și modele în evoluția amenințărilor la nivel național și internațional
CG 6. Analiza factorilor care condiționează asigurarea securității informaționale.	RÎ10. analiza datelor sensibile și informațiilor relevante privind respectarea legislației și transparența față de public în domeniul securității informaționale
COMPETENȚE PROFESIONALE (CP)	REZULTATELE ÎNVĂȚĂRII (RI)
CP 2. Implementarea strategiilor și direcțiilor în asigurarea securității informaționale la nivel internațional	RÎ13. dezvolta strategii globale de asigurare a securității informaționale
CP7. Consiliere în realizarea activităților instituțiilor și organizațiilor responsabile de securitatea informațională la nivel național, regional și internațional.	RÎ18. elabora studii, evaluări, rapoarte și scenarii pentru aprecierea subiectelor și incidentelor de securitate informațională
CP8. Eficientizarea managementului activității instituțiilor și organizațiilor în gestionarea eficientă a provocărilor și riscurilor de securitate informațională	RÎ19. planifica activitățile instituțiilor și organizațiilor responsabile de securitatea informațională; determina rolul statului în gestionarea problemelor de securitate informațională
CP 9. Gestionarea crizelor și conflictelor informaționale	RÎ20. identifica riscurile și amenințările în gestionarea crizelor informaționale; identifica opțiuni de consolidare a sectorului securității naționale împotriva amenințărilor și conflictelor hibride
CP 10. Modelarea tehnologiilor moderne și informațiilor digitale de comunicare strategică și de criză	RÎ22. aplica tehnici de comunicare strategică și gestionare a situațiilor de criză; elabora și dezvolta studii prospective, analizând tendințe actuale și viitoare
CP 11. Prognozarea tendințelor și impactului acțiunilor, deciziilor și proceselor de coordonare internă și de cooperare internațională în domeniul securității informaționale	RÎ23. evalua tendințe, amenințări, și perspective solide asupra evoluțiilor de securitate informațională; identifica potențialele amenințări și vulnerabilități în contextul securității informaționale
CP. 13. Interpretarea procesului de cooperare și comunicare strategică și de criză	RÎ25. asigura analiza procesului de comunicare strategică între sectorul de securitate al Republicii Moldova, mediului științific și societatea civilă
CP. 13 Interpretarea procesului de cooperare și comunicare strategică și de criză	RÎ26. evalua comunicarea strategică și de criză
CP14. Realizarea analizelor impactului războiului informațional și studiilor prospective	RÎ27. asigura interpretarea datelor, elabora și dezvolta scenarii prospective, analizând tendințele actuale și viitoare

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

III. UNITĂȚI DE ÎNVĂȚARE

Tema 1. ISTORIOGRAFIA, BAZELE TEORETICO-CONCEPTUALE ȘI METODOLOGICE ALE CERCETĂRII SECURITĂȚII INFORMAȚIONALE		
Rezultatele învățării preconizate a fi atinse: RI 1; RI 10; 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. Fundamentele istoriografiei cercetării securității informaționale; 2. Teorii și conceptualizări în cercetarea securității informaționale; 3. Rolul securității informaționale în realizarea securității naționale a statului.	- Relatează despre istoriografia cercetării securității informaționale; - Utilizează metodologii de analiză aplicativă a situației internaționale; - Explică importanța teoretică și practică al programului; - Definește noțiunea de “securitate informațională”; - Evaluează rolul securității informaționale, importantă resursă pentru organizații responsabile de luarea deciziilor.	Absolventul în mod autonom și responsabil elaborează metodologii 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 1; RI 10; RI 13; 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; 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. - Evaluează politica de securitate a informației în cadrul instituțiilor publice și metodologia cercetării.	Absolventul în mod responsabil și autonom analizează surse și formulează concluzii bine fundamentate 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.
Tema 3. PROTECȚIA INFORMAȚIEI. PREVENIREA ȘI CURMAREA FRAUDELOR INFORMATICE		
Rezultatele învățării preconizate a fi atinse: RI 1; RI 10; RI 18		

Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>securitate informațională, știri false, mediului informațional, pericol, politică.</i> Unități de conținut: 1. Situația mediului informațional privind protecția informațiilor sensibile și infrastructurii critice; 2. Procesul de comunicare strategică între sectorul de securitate a Republicii Moldova, mediului științific și societatea civilă; 3. Analiza factorilor care condiționează asigurarea securității informaționale.	- Definește caracteristicile securității informaționale; - Determină instrumentele și metodele de luptă cu amenințările cibernetice; - Explică motivele criminalității cibernetice; - 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 1; RI 7; RI 9; RI 22

Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>colaborare, securitate informațională, programe internaționale, acorduri, negocieri.</i> Unități de conținut: 1. Căile de colaborare a instituțiilor responsabile de securitatea informațională 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. 4. Activitatea la programe internaționale care vizează domeniul securității informaționale.	- Identifică căile de colaborare internațională a instituțiilor responsabile de securitatea informațională în domeniul prevenirii și combaterii terorismului și criminalității transfrontaliere; - 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; - Evaluează activitatea la programe internaționale care vizează domeniul securității informaționale.	Absolventul în mod autonom poate aplica cadrul normativ și analiza provocărilor globale, precum și atacurile cibernetice transfrontaliere și necesitatea unor răspunsuri coordonate la nivel internațional; 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 ; RI 10; RI 13; RI 22		
Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>securitate informațională, război informațional, mediu informațional, pericol, politică.</i> Unități de conținut: 1. Geneză și trăsăturile războiului informațional; 2. Forme de manifestare, practici și strategii ale actorilor internaționali împotriva războiului informațional și procesul de asigurare a securității naționale și internaționale; 3. Impactul războiului informațional asupra securității naționale a Republicii Moldova.	- 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. - Utilizează 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 ACTIVITATEA SERVICIILOR DE INFORMAȚII ÎN CONTEXTUL GLOBALIZĂRII		
Rezultatele învățării preconizate a fi atinse: RI 2; RI 22; RI 23		
Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>Republica Moldova, sectorul de securitate, reziliență, riscuri, amenințări, vulnerabilități de securitate, capacitate de reziliență și răspuns, cultura de securitate.</i> Unități de conținut: 1. Reziliența din perspectiva securității informaționale: aspecte teoretice și practice; 2. Reziliență strategică: de la stabilitate și prevenție la acțiune pro-activă și adaptabilitate dinamică; 3. Opțiuni de consolidare a sectorului securității naționale împotriva amenințărilor și conflictelor	- Identifică activitatea serviciilor de informații în contextul globalizării; - Relatează despre securitatea informațională ca factor de organizare a societății contemporane; - Evaluează riscurile și amenințările la adresa securității informaționale; - Analizează cadrul de cooperare pe arena internațională în domeniul securității informațiilor a serviciilor/agențiilor/ comunităților de informații; - Elaborează noi responsabilități pe conlucrare a serviciilor de informații ce țin de dezvoltarea unei colaborări eficiente privind creșterea transparenței instituționale.	Absolventul poate în mod autonom gestiona și analiza scenarii de conflict, utilizând trinomul vulnerabilitate-risc-amenințare și de a corela problemele fundamentale și fenomenele asociate cu riscurile, vulnerabilitățile și amenințările la adresa securității; evalua protecția datelor 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.

hibride.		
Tema 7. SECURITATEA INFORMAȚIONALĂ ȘI TERORISMUL – PREOCUPARE GLOBALĂ Rezultatele învățării preconizate a fi atinse: RI 1; RI 13; RI 18; RI 20		
Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>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.</i> Unități de conținut: 1. Conceptul și tipologii ale terorismului internațional; 2. Provocările actuale în domeniul securității informaționale; 3. Eficiența și rolul colaborării internaționale a serviciilor de informații în domeniul prevenirii și combaterii terorismului;	- Relatează despre istoriografia cercetării securității informaționale și terorismului; - Definește noțiunea de securitate informațională, noțiunea de terorism; - Estimează provocările actuale în domeniul securității informaționale; - Explică poziția actorilor internaționali pe subiecte relevante pentru agenda internațională; - Propune tehnici de comunicare strategică în vederea depășirii crizelor; - 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.
Tema 8. ISLAMUL RADICAL. MECANISME DE RECRUTARE ÎN MEDIUL ONLINE Rezultatele învățării preconizate a fi atinse: RI 1; RI 9; RI 17; RI 22		
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.</i> Unități de conținut: 1. Instrumente și mecanisme de prevenire a radicalizării și oclotirii valorilor, garantării securității	- Identifică instrumentele și mecanismele de prevenire a radicalizării și oclotirii valorilor, garantării securității cetățenilor în spațiul virtual; - Explică poziția actorilor internaționali pe subiecte relevante pentru agenda internațională; - Evaluează și determină metodele de radicalizare a islamaștilor prin intermediul rețelelor;	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.

cetățenilor în spațiul virtual; 2. Metode de radicalizare a islamiștilor prin intermediul rețelelor; 3. Scopuri teroriste online prin intermediul propagandei și radicalizării care conduc la terorism în mediul online.	- Analizează scopurile teroriste online prin intermediul propagandei și radicalizării care conduc la terorism în mediul online.	
Tema 9. SECURITATEA INFORMAȚIONALĂ LA NIVEL EUROPEAN Rezultatele învățării preconizate a fi atinse: RI 1; RI 10; RI 13; RI 22		
Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>nivel european, protecția informației, amenințări cibernetice, schimb de informații, frontiere externe.</i> Unități de conținut: 1. Nevoia implementării unei strategii proactive pentru protejarea spațiului informațional european; 2. Elaborarea și implementarea unei reforme legislative la nivel European care ar îngloba responsabilitatea statelor pentru crimele cibernetice. 3. Acțiunile UE în sporirea schimbului de informații, intensificarea verificărilor la frontierele externe, îmbunătățirea controalelor armelor de foc, digitalizarea cooperării judiciare prevenirea radicalizării online, blocarea finanțării terorismului și altele.	- Defiște caracteristicile terorismului informațional în spațiul european; - Determină instrumentele și metodele de luptă cu amenințările cibernetice; - Influențează implementarea acțiunilor UE în sporirea schimbului de informații, intensificarea verificărilor la frontierele externe; - Propune tehnici de comunicare strategică în vederea depășirii crizelor; - explică poziția actorilor internaționali pe subiecte relevante pentru agenda internațională; - îmbunătățirea controalelor armelor de foc, digitalizarea cooperării judiciare, prevenirea radicalizării online, blocarea finanțării terorismului și altele. - Evaluează motivele criminalității informaționale; - Analizează eforturile întreprinse pentru asigurarea securității informațiilor și de securitate națională, în general.	Absolventul în mod autonom dezvoltă strategii de gestionare a conflictelor și crizelor europene; interpretează și evaluează datele privind evoluțiile la nivel european; dezvoltă strategii de gestionare a spațiului informațional european.
Tema 10. PERICOLUL ȘTIRILOR FALSE ASUPRA SECURITĂȚII INFORMAȚIONALE Rezultatele învățării preconizate a fi atinse: RI 1; 10; RI 18; RI 22		
Cunoștințe/unități de conținut	Abilități	Responsabilitate și autonomie
Termeni-cheie: <i>securitate informațională, știri false, mediului informațional, pericol, politică.</i> Unități de conținut 1. Situația mediului informațional privind protecția informațiilor sensibile	- Identifică situația mediului informațional privind protecția informațiilor sensibile și infrastructurii critice; - Analizează evoluția fenomenului știrilor false și dezinformării la nivel național și internațional; - Estimează combaterea știrilor false și	Masterandul poate în mod autonom evalua riscurile specifice afacerilor externe și identifică soluții eficiente pentru depășirea acestora; dezvoltă strategii de gestionare a pericolelor, conflictelor și crizelor internaționale; supraveghează și controlează respectarea legilor și a

și infrastructurii critice; 2. Procesul de comunicare strategică între sectorul de securitate a Republicii Moldova, mediului științific și societatea civilă; 3. Elucidarea aspectelor combaterii știrilor false și identificarea eficientă a căilor de soluționare a acestora în condițiile provocărilor de securitate.	dezinformării de către stat între cenzură și drepturile omului; -Evaluează măsurile necesare aplicabile combaterii știrilor false în contextual situației pandemice actuale; - Elucidează aspectele combaterii știrilor false; - Identifică eficiența căilor de soluționare a provocărilor de securitate.	drepturilor individuale în domeniul securității informaționale.
--	--	---

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

IV. STUDIUL INDIVIDUAL AL STUDENTULUI

Nr.	Produsul preconizat	Strategii de realizare	Criterii de evaluare	Termen de realizare
1.	Proiect de cercetare: Rolul securității informaționale în conflictele hibride moderne	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 acesteia 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	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	Pe parcursul semestrului

		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 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	- Relevanța concluziilor	
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 anumitor 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 (specifice disciplinei)

Tehnologiile și strategiile didactice aplicate în predarea 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 II, 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%

V. BIBLIOGRAFIE RECOMANDATĂ:

Pe suport de hârtie

1. 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.
2. 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.
3. 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.
4. Busuncian T. Radical Islam. Recruitment Mechanisms in Immediate Neighborhood with European Union. spre publicare 2019, responsabil Teosa V.
5. 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.
6. A History of Cyberspace. Per Concordiam, v. 7, nr. 2, 2016.
7. Bar-Zohar M., Misal N. Mossad. Istoria sângeroasă a spionajului Izraelian. București 2019, 414 p.
8. Friedman M. Spioni fără țară. Vieți secrete în momentul nașterii statului Israel, București, 2019, 267 p.
9. Chaliand G., Blin A. Istoria terorismului. Din antichitate până la Daesh. București, Polirom, 2018, 575 p.
10. Hughes-Wilson_J. Serviciile secrete (Titlu original: On Intelligence). București, Meteor Publishing, 2017, 496 p.
11. Ruben Tuitel. Defining Cyber Terrorism Concordiam, V7, Nr. 2, 2016, pp. 10-17.
12. Terrorist attacks in Europe highlight the need to monitor European extremists fighting abroad. Concordiam, V6, Nr.2, 2015, pp. 61-63.
13. Eveniment științifico-practic organizat de Institutul Național de Informații și Securitate ”Bogdan Întemeietorul Moldovei”
14. Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică. București 2004, 71 p.
15. Hotărârea Guvernului Nr. 746 din 18.08.2010 "Cu privire la aprobarea Planului Individual de Acțiuni al Parteneriatului Republica Moldova – NATO actualizat". Monitorul Oficial al Republicii Moldova No. 166-168 din 14.09.2010
16. Hughes-Wilson J. Serviciile secrete. București: Meteor Publishing, 2017, pag. 17-18
17. Legea nr. 286/2009 privind noul Cod Penal, publicată în Monitorul Oficial nr. 510 din 24 iulie 2009, în vigoare de la 1 februarie 2014.
18. Born H., Wills A. Supravegherea serviciilor de informații. Set de instrumente. DCAF, Geneva, 2012. 273 p.
19. Tielidze G., Bagge D., Spinu N. and Ivanović Z. Regional Cyber Security. B: per Concordiam, Vol. 5, issue 2, 2014. p. 24-34.
20. Initiative de contracarare a banilor publici, Chisinau, 2015, 86 p.
21. Мазуров В. Кибертерроризм: понятие, проблемы противодействия. Доклады ТУСУРа, № 1 (21), ч. 1, июнь 2010. с. 41–44.
22. Смирнов А. Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза. Москва: ЮНИТИ-ДАНА, 2011.

23. Шрайер Ф., Викс Б., Винклер Т. Кибербезопасность: дорога, которую предстоит пройти. Женева: Женевский Центр демократического контроля над вооруженными силами, 2013. 62 с.

Surse electronice:

1. Busuncian T. Colaborarea organelor securității statului ale Republicii Moldova în combaterea terorismului pe plan interdepartamental și internațional. În: „Arhitectura Securității în Vecinătatea Estică a UE: Provocări și Realități”, Chișinău, 2011, p. 162-170.
http://www.soros.md/files/publications/documents/CARTEA_final_ro.pdf
2. Advances in Cyber Security Analytics and Decision Systems.
Shishir K Shandilya editor (Editor) <http://idlogov/vocabulary/relators/edt>; Neal Wagner editor (Editor) <http://idlogov/vocabulary/relators/edt>; Atulya K Nagar editor (Editor) <http://idlogov/vocabulary/relators/edt>, 2020; 1st ed. 2020.
3. Hibberd G. The Art of Cyber Security: A Practical Guide to Winning the War on Cyber Crime, 2022; 1 st 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
4. Hotărâre 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
5. Hotărârea guvernului Nr. 414 din 08.05.2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat Publicat în Monitorul Oficial Nr. 157-166. <http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=375459>
6. Hotărârea Nr. 257 din 22-11-2018 privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 și a Planului de acțiuni pentru implementarea acesteia Publicat: Monitorul Oficial al Republicii Moldova Nr. 13-21 din 18-01-2019.
https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro
<http://www.academy.police.md/22> (vizitat: 19.02. 2021).
7. Institutul Național de Informații și Securitate. <https://www.sis.md/ro/content/institutul-na%C5%A3ional-de-informa%C5%A3ii-%C5%9Fi-securitate>
8. Înșelăciune prin sisteme informatice, fraudă informatică și fals informatic. Percheziții domiciliare <http://www.juridice.ro/295789/diicot-inselaciune-prin-sisteme-informatice-frauda-informatic-si-fals-informatic-perchezitii-domiciliare.html>
9. Legea Nr. 299 din 21-12-2017 privind aprobarea Concepției securității informaționale a Republicii Moldova. Publicat: Monitorul Oficial al Republicii Moldova Nr. 48-57 din 16-02-2018.
https://www.legis.md/cautare/getResults?doc_id=105660&lang=ro
10. Materialele mesei rotunde ”Combaterea știrilor false în condițiile provocărilor de securitate COVID-19”. Măsuri executorii privind înlăturarea cauzelor și condițiilor ce contribuie la realizarea amenințărilor securității de stat <https://sis.md/ro/content/m%C4%83suri-executorii-privind-%C3%AEEnl%C4%83turarea-cauzelor-%C8%99i-condi%C8%9Biilor-ce-contribuie-la-realizarea>
11. Războiul electronic și inteligența artificială, 2024.
https://www.researchgate.net/publication/377248415_Razboiul_electronic_si_inteligența_artificială
12. Un site care publică informații false despre Covid-19 va fi sistat. <https://www.sis.md/ro/content/un-site-care-public%C4%83-informa%C5%A3ii-false-despre-covid-19-va-fi-sistat>