**UNIVERSITATEA DE STAT DIN MOLDOVA**

**FACULTATEA RELAŢII INTERNAŢIONALE, ŞTIINŢE POLITICE ŞI ADMINISTARTIVE**

**DEPARTAMENTUL RELAŢII INTERNAŢIONALE**

# CURRICULUM

la disciplina

# „ Securitatea Informațională”

## Ciclul I, MASTERAT
## Specialitatea Studii Diplomatice

**AUTOR:**

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

**APROBAT**
**la şedinţa Departamentului**
**din „ ____” _____ 2025**
**proces-verbal nr. _____**
**Şef Departament_____**

**APROBAT**
**la şedinţa 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 internaţionale tratate ca sistem, concepte, categorii și strategii ale securității informaționale contemporane.

**Locul şi 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 şi ştiinţifico-aplicativ deosebit de important pentru aprofundarea familiarizării masteranzilor cu cerințele de cercetare științifică în domeniul relațiilor internaţionale, 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 procedeelor şi metodelor acestora pentru a familiariza masteranzii despre rolul şi importanța securității informaționale în realizarea politicii interne și externe a statelor. Programul presupune o incursiune profundă în noțiunile conexe și concurente privind dimensiunea structural-funcţională a securității informaționale în noul context de securitate din perspectiva eficacității formelor colaborării internaţionale, inclusiv a organelor securității statului din Republica Moldova. Studierea 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 învăţământ | 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 | | asincron* | individual | | |
| cu frecvenţă | S.A.10 | *Securitatea Informațională* | *Busuncian Tatiana* | **II** | **180** | **15** | **30** | **135** | | | | **Ex.** | **6** |
| cu frecvenţă redusă | | | | | | | | | | | | | |
| la distanță | | | | | | | | | | | | | |
| cu frecvență *dual* | | | | | | | | | | | | | |

*formare profesională practică la unitate - pentru învățământul dual

*pentru învățământul cu frecvență redusă și la distanță

## II. TEMATICA ŞI REPARTIZAREA ORIENTATIVĂ A ORELOR

| Nr. d/o | Unităţi de conţinut | 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 informaţiei. Prevenirea şi 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** | | | | | | | | | **135** | | | | | |

## III. COMPETENŢE GENERALE, PROFESIONALE ŞI REZULTATELE ÎNVĂȚĂRII

| **COMPETENȚE GENERALE (CG)** | **REZULTATELE ÎNVĂȚĂRII (RI)**<br>***Absolventul/candidatul la atribuirea calificării poate*** |
|---|---|
| **CG 1. Analiza şi compararea capacităților de dezvoltare şi consolidare a sistemului național de securitate** | **RI 1 stabili cadrul teoretic și practic în contextul evoluțiilor problematicii analizei interdisciplinare a dimensiunii informaționale;** |
| **CG 6. Elabora politici și strategii de securitate națională** | **RI 10 interpreta esența și specificul analizei științifice în domeniul securității informaționale.** |
| | |
| **COMPETENȚE PROFESIONALE (CP)** | **REZULTATELE ÎNVĂȚĂRII (RI)** |
| **CP 2. Formula propuneri şi recomandări privind eficientizarea asigurării securității naționale** | **RI 7 implementa programe și politici eficiente pentru a influența în mod pozitiv procesul politic** |
| **CP7. Consiliere în realizarea activităților instituțiilor şi organizațiilor responsabile de politica externă și internațională** | **RI 9 facilita dialogul, cooperarea și comunicarea instituțională;** |
| **CP 9. Gestionarea crizelor și conflictelor politice** | **RI 13 formula standarde regionale și globale pentru utilizarea celor mai bune practici în domeniul securității informaționale;** |
| **CP 10. Modelarea tehnologiilor politice și comunicării strategice și de criză** | **RI 17 dezvolta propuneri de proiecte și politici pe subiectele relevante din domeniul securității informaționale;** |
| **CP 11. Prognozarea tendințelor și impactului acțiunilor, deciziilor și proceselor politice** | **RI 18 elabora studii, evaluări, rapoarte și scenarii pentru aprecierea subiectelor de politică externă și internațională;** |
| **CP. 13 Elaborarea politicilor și strategiilor de securitate națională** | **RI 20 determina formele analitico-aplicative de analiză a dimensiunii militare a securității** |
| **CP14 Realizarea analizelor politice și studiilor prospective** | **RI 22 aplica tehnici de comunicare strategică și gestionare a situațiilor de criză** |

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

## III. UNITĂŢI DE ÎNVĂŢARE

| **Tema 1. ISTORIOGRAFIA CERCETĂRII SECURITĂȚII INFORMAȚIONALE**<br><br>**Rezultatele învățării preconizate a fi atinse: RI 1; RI 10; RI 18** | | |
|---|---|---|
| **Cunoștințe/unități de conținut** | **Abilități** | **Responsabilitate și autonomie** |
| **Termeni-cheie:**<br>*securitate informațională; securitatea informației, securitate cibernetică, noțiuni, instrumente, stat.*<br><br>**Unități de conținut:**<br>1. Istoriografia cercetării securității informaționale, obiectul de studiu, structura cursului, sursele bibliografice pe domeniul securității informaționale;<br>2. Locul cursului printre alte discipline din domeniul programului ”Studii de securitate și Managementul Informației”, importanța teoretică și practică a studiului;<br>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;<br><br>- Dezvoltă obiectul de studiu și structura cursului;<br><br>- Proiectează locul și rolul cursului printre alte discipline din domeniul programului ”Studii de securitate și Managementul Informației”, importanța teoretică și practică al programului;<br><br>- Definește noțiunea de “securitate informațională”;<br><br>- 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**<br><br>**Rezultatele învățării preconizate a fi atinse: RI 1; RI 10; RI 18;** | | |
| Cunoștințe/unități de conținut | Abilități | Responsabilitate și autonomie |
| **Termeni-cheie:**<br>*securitate informațională, concepte, noțiuni, riscuri, crime, fraude, război informațional, stat, etc.*<br><br>**Unități de conținut:**<br>1. Concepte și noțiuni privind securitatea informațională;<br>2. Evoluția și accesul la tehnologia informației - un număr tot mai mare de incidente cibernetice motivate politic împotriva securității statelor;<br>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;<br><br>- Determină rolul statului în gestionarea problemelor de securitate informațională;<br><br>- Estimează riscurile, crimele și fraudele informaționale;<br><br>- Evaluează politica de securitate a informației în cadrul instituțiilor publice | 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. |

| | | |
|---|---|---|
| | și metodologia cercetării. | |

**Tema 3. PROTECȚIA INFORMAȚIEI. PREVENIREA ȘI CURMAREA FRAUDELOR INFORMATICE**

**Rezultatele învățării preconizate a fi atinse: RI 1; RI 10; RI 18; RI 22**

| Cunoștințe/unități de conținut | Abilități | Responsabilitate și autonomie |
|---|---|---|
| **Termeni-cheie:**<br>*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 cibernetice, măsuri tehnice de securitate cibernetică, actualizarea i patch-urile software, backup-uri și planuri de recuperare în caz de dezastru.*<br><br>**Unități de conținut:**<br>1. Protecția informațiilor sensibile și infrastructurii critice, asigurarea securității informaționale;<br>2. Procesul de comunicare strategică între sectorul de securitate al Republicii Moldova, mediului științific și societatea civilă;<br>3. Elucidarea aspectelor combaterii știrilor false și identificarea eficientă a căilor de soluționare a acestora în condițiile provocărilor de securitate. | - Definește caracteristicile securității informaționale;<br><br>- Determină instrumentele şi metodele de luptă cu amenințările cibernetice;<br><br>- Evaluează motivele criminalității cibernetice şi descrie eforturile întreprinse pentru asigurarea securității informaționale şi de securitate națională, în general;<br><br>- 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 17; RI 18; RI 20**

| Cunoștințe/unități de conținut | Abilități | Responsabilitate și autonomie |
|---|---|---|
| **Termeni-cheie:**<br>*colaborare, securitate informațională, programe internaționale, acorduri, negocieri.*<br>**Unități de conținut:**<br>1. 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;<br>2. Inițierea negocierilor privind semnarea acordurilor de cooperare la nivel internațional pentru îmbunătățirea capacității de răspuns în cazul unor atacuri cibernetice majore;<br>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;<br><br>- 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**<br><br>**Rezultatele învățării preconizate a fi atinse: RI 1; RI 10; RI 13; RI 22** | | |
| **Cunoștințe/unități de conținut** | **Abilități** | **Responsabilitate și autonomie** |
| **Termeni-cheie:**<br>*securitate informațională, război informațional, mediu informațional, pericol, politică.*<br><br>**Unități de conținut:**<br>1. Istoriografia cercetării războiului informațional, geneza și trăsăturile războiului informațional;<br>2. Forme de manifestare pe arena internațională, practici și strategi ale actorilor internaționali împotriva războiului informațional și procesul de asigurare a securității naționale și internaționale;<br>3. 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;<br><br>- Determină forme de manifestare pe arena internațională;<br><br>- Evaluează practici și strategi ale actorilor internaționali împotriva războiului informațional și în procesul de asigurare a securității naționale și internaționale;<br><br>- Analizează impactul războiului informațional asupra securității naționale a Republicii Moldova;<br><br>- Estimează practici și instrumente de luptă a Republicii Moldova împotriva războiului informațional. | Absolventul în mod autonom poate identifica metodele de propagandă și manipulare in 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 infirmaționale (educație, media, gândire critică).<br>. |
| **Tema 6. SECURITATEA INFORMAȚIONALĂ ȘI ACTIVITATEA SERVICIILOR DE INFORMAȚII ÎN CONTEXTUL GLOBALIZĂRII**<br><br>**Rezultatele învățării preconizate a fi atinse: RI 1; RI 9; RI 17; RI 22** | | |
| **Cunoștințe/unități de conținut** | **Abilități** | **Responsabilitate și autonomie** |
| **Termeni-cheie:**<br>*Sectorul de securitate, reziliență, riscuri, amenințări, vulnerabilități de securitate, capacitate de reziliență și* | - Identifică activitatea serviciilor de informații în contextul globalizării;<br><br>- Relatează despre adaptarea serviciilor | Masterandul poate în mod autonom gestiona și analiza scenarii de conflict, utilizând trinomul vulnerabilitate-risc- |

| | | |
|---|---|---|
| *răspuns, cultura de securitate, riscurile cibernetice, măsuri tehnice de securitate cibernetică, actualizarea i patch-urile software, backup-uri și planuri de recuperare în caz de dezastru.*<br><br>**Unități de conținut:**<br>1.Activitatea serviciilor de informații în contextul globalizării și adaptarea acestora la noile riscuri și amenințări la adresa securității informaționale;<br>2. Cooperare pe arena internațională în domeniul securității informaționale a serviciilor/agențiilor/ comunităților de informații;<br>3. Conlucrarea serviciilor de informații în dezvoltarea colaborării eficiente privind creșterea transparenței instituționale. | de informații la noile riscuri și amenințări la adresa securității informaționale;<br><br>- Analizează cadrul de cooperare pe arena internațională în domeniul securității informaționale a serviciilor/agențiilor/ comunităților de informații;<br><br>- Elaborează noi responsabilități pe conlucrare a serviciilor de informații ce ține 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 1; RI 9; RI 13; RI 20**

| Cunoștințe/unități de conținut | Abilități | Responsabilitate și autonomie |
|---|---|---|
| **Termeni-cheie:**<br>*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.*<br><br>**Unități de conținut:**<br>1. Istoriografia cercetării securității informaționale, noțiunea de securitate informațională și terorism; | - Relatează despre istoriografia cercetării securității informaționale;<br><br>- Definește noțiunea de securitate informațională, noțiunea de terorism;<br><br>- Estimează provocările actuale în domeniul securității informaționale;<br><br>- 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;<br>3. Colaborarea internațională a serviciilor de informații în domeniul prevenirii și combaterii terorismului. | | |
| **Tema 8. ISLAMUL RADICAL. MECANISME DE RECRUTARE ÎN MEDIUL ONLINE**<br><br>**Rezultatele învățării preconizate a fi atinse: RI 1; RI 7; RI 9; RI 22** | | |
| **Cunoștințe/unități de conținut** | **Abilități** | **Responsabilitate și autonomie** |
| **Termeni-cheie:**<br>*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.*<br><br>**Unități de conținut:**<br>1. Instrumente și mecanisme de prevenire a radicalizării și și ocrotirii valorilor, garantării securității cetățenilor în spațiul virtual.<br>2. Evaluarea și determinarea metodelor de radicalizare a islamiștilor prin intermediul rețelelor.<br>3. Scopuri teroriste online prin intermediul propagandei și radicalizării care conduc la terorism în mediul online. | - Identifică instrumentele și mecanismele de prevenire a radicalizării și ocrotirii valorilor, garantării securității cetățenilor în spațiul virtual;<br><br>- Evaluează și determină metodele de radicalizare a islamiștilor prin intermediul rețelelor;<br><br>- 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.*

## IV. STUDIUL INDIVIDUAL AL STUDENTULUI

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

| | | | | |
|---|---|---|---|---|
| | | - Evaluarea legăturii dintre aspectele teoretice și cele practice ale relațiilor internaționale<br>- Proiectarea noului sistem de securitate informațională.<br><br>**Modalități de prezentare:**<br>*În scris* – 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 *verbal* – 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.<br>• Evaluarea impactului transformărilor asupra mediului de securitate internațional. | | ***La sfârșitul semestrului*** |
| **3.** | **Simulări și studii de caz** pentru aplicarea cunoștințelor teoretice.<br><br>**Dezbateri:**<br>Opțiuni de consolidare a sectorului securității naționale împotriva amenințărilor și conflictelor hibride<br><br>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***<br>- Diversitatea surselor.<br>- Analiza critică a rezultatelor prezentate.<br>- Identificarea posibilităților de aplicare a rezultatelor.<br>- Relevanța concluziilor.<br>- Originalitatea formei de prezentare. | ***Pe parcursul semestrului*** |

## VI. SUGESTII METODOLOGICE DE PREDARE-ÎNVĂȚARE-EVALUARE

- **Formele de organizare a instruirii:**

Formele principale ale instruirii sunt cursul şi seminarul. Cursul este organizat sub formă de prelegere clasică, dezbatere, poate fi curs mixt prelegere – dezbatere, curs practic – aplicativ, prelegere problematizată. Seminarul de asemenea are mai multe forme: seminare de reluare şi aprofundare a anumitelor probleme abordate în cadrul cursului, de realizare a corelaţiilor intra-inter şi transdisciplinare; dezbatere, braistorming, 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 si strategiile didactice aplicate în predare cursului se instituie atât in raport de implicație cât şi de complementaritate funcţionala. Astfel, strategiile şi tehnologiile didactice aplicate sunt expunerea didactică, conversația didactică, demonstrația, lucrul cu actele normative, modelarea didactica, 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 şi finală.

1. Evaluarea inițială/diagnostică, orală se efectuează le începutul activităţilor de predare pentru a stabili gradul de pregătire a masteranzilor pentru cursul preconizat, potenţialul de învăţare la începutul unei noi activităţi. Se apreciază prin *interviu, chestionare orală, conversaţie, expuneri orale*, cunoştinţele, abilităţile şi competenţele profesionale formate pe parcursul ciclului I, pentru a şti dacă sunt apţi să se integreze cu şanse de reuşită 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), şi *lucrări de laborator*, cu scopul de a cunoaşte dacă şi în ce măsură obiectivele privind cunoştinţele şi capacităţile ce trebuiau însuşite au fost atinse. Demersul vizează atât cunoașterea progreselor masterandului, cât şi identificarea dificultăţilor de învăţare 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% |
| - activităţi practice | | 0% |
| - alte activităţi (precizaţi) | | 0% |
| rezultatele de la examenul final | **cel mult 40%** | 40% |

## BIBLIOGRAFIE RECOMANDATĂ:

**Pe suport de hârtie**


1. 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.
2. 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.
3. Busuncian T. Parametrii instituționali ai securităţii informaționale. Materialele conferinței ştiinţifico-practice naționale „Mandatul de securitate: probleme actuale de interpretare, legislaţie şi practică". Serviciul de Informaţii şi Securitate al Republicii Moldova Institutul Naţional de Informaţii şi Securitate „Bogdan, Întemeietorul Moldovei". Chișinău, 2020, p. 71-75.
4. 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.

5. 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
6. 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.
7. A History of Cyberspace. Per Concordiam, v. 7, nr. 2, 2016.
8. Bar-Zohar M., Misal N. Mossad. Istoria sângeroasă a spionajului Izraelian. București 2019, 414 p.
9. Friedman M. Spioni fără țară. Vieți secrete în momentul nașterii statului Israel, Bucureșri, 2019, 267 p.
10. Chaliand G., Blin A. Istoria terorismului. Din antichitate până la Daesh. Bucureşti, Polirom, 2018, 575 p.
11. Hughes-Wilson_J. Serviciile secrete (Titlu original: On Intelligence). București, Meteor Publishing, 2017, 496 p.
12. Ruben Tuitel. Defining Cyber Terrorism Concordiam, V7, Nr. 2, 2016, pp. 10-17.
13. Terrorist attacks in Europe highlight the need to monitor European extremists fighting abroad. Concordiam, V6, Nr.2, 2015, pp. 61-63.
14. Eveniment științifico-practic organizat de Institutul Național de Informații și Securitate ”Bogdan Întemeietorul Moldovei”
15. Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică. București 2004, 71 p.
16. 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
17. Hughes-Wilson J. Serviciile secrete. București: Meteor Publishing, 2017, pag. 17-18
18. 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.
19. Born H., Wills A. Supravegherea serviciilor de informaţii. Set de instrumente. DCAF, Geneva, 2012. 273 p.
20. Tielidze G., Bagge D., Spinu N. and Ivanović Z. Regional Cyber Security. B: per Concordiam, Vol. 5, issue 2, 2014. p. 24-34.
21. Initiative de contracarare a banilor publici, Chisinau, 2015, 86 p.
22. Мазуров В. Кибертерроризм: понятие, проблемы противодействия. Доклады ТУСУРа, № 1 (21), ч. 1, июнь 2010. с. 41–44.
23. Смирнов А. Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза. Москва: ЮНИТИ-ДАНА, 2011.
24. 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. Amenințările de Manipulare și Interferență a Informațiilor Externe. https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf
2. Busuncian T. Colaborarea organelor securităţii statului ale Republicii Moldova în combaterea terorismului pe plan interdepartamental şi internaţional. În: „Arhitectura Securităţii în Vecinătatea Estică a UE: Provocări şi Realităţi”, Chişinău, 2011, p. 162-170. http://www.soros.md/files/publications/documents/CARTEA_final_ro.pdf
3. Advances in Cyber Security Analytics and Decision Systems.

Shishir K Shandilya editor (Editor) http://idlocgov/vocabulary/relators/edt; Neal Wagner editor (Editor) http://idlocgov/vocabulary/relators/edt; Atulya K Nagar editor (Editor) http://idlocgov/vocabulary/relators/edt, 2020; 1st ed. 2020.
4. 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=alma991241771469057 63&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. 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
6. 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
7. 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).
8. Institutul Național de Informații și Securitate. https://www.sis.md/ro/content/institutul-na%C5%A3ional-de-informa%C5%A3ii-%C5%9Fi-securitate
9. 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
10. 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
11. 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%AEnl%C4%83turarea-cauzelor-%C8%99i-condi%C8%9Biilor-ce-contribuie-la-realizarea
12. Războiul electronic și inteligența artificială, 2024. https://www.researchgate.net/publication/377248415_Razboiul_electronic_si_inteligenta_artificiala
13. 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