MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
Lesya Ukrainka Volyn National University
International Relations Faculty
International Relations Department

SYLLABUS

of an elective academic component

«MODERN INTERNATIONAL ORGANIZATIONS IN THE FIELD OF INFORMATION SECURITY»

Bachelor training

Lutsk – 2026

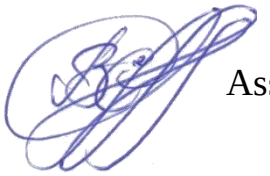
The syllabus of the elective academic component «Modern International Organizations in the Field of Information Security», Education Level – Bachelor.

Developer: PhD of 291 «International Relations, Public Communications and Regional Studies», senior lecturer of the International Relations Department, **Nazarii SHULIAK**

Approved
by the Guarantor of the Education and Professional Programme:

Associate professor **Yevhenia VOZNIUK**

The syllabus of the elective academic component was approved at the meeting of the International Relations Department
Protocol № 7 of January 30, 2026.

Head of the Department:  Associate professor **Yevheniia VOZNIUK**

©Shuliak N., 2026

I. THE DESCRIPTION OF THE ELECTIVE ACADEMIC COMPONENT

<table>
<tr><th>Indicator Name</th><th>Field of Knowledge, Educational and Professional Programme, Education Level</th><th>Characteristics of the Academic Component</th></tr>
<tr><td rowspan="2">Full-Time Form of Education</td><td rowspan="7">C «Social Sciences, Journalism, Information and International Relations»,
C3 «International Relations», «International Communication and Mediation»,
bachelor</td><td>Elective</td></tr>
<tr><td>Year of Study – 2</td></tr>
<tr><td>Number of Hours / Credits
150 / 5</td><td>Semester – 3</td></tr>
<tr><td rowspan="2">Lectures – 10 hours</td></tr>
<tr><td>Seminars – 20 hours</td></tr>
<tr><td>Individual Student’s Work:
no</td><td>Independent Work – 110 hours</td></tr>
<tr><td colspan="2"></td><td>Consultations – 10 hours</td></tr>
<tr><td colspan="2"></td><td>Form of Control: Credit</td></tr>
<tr><td colspan="2">Language of Study:</td><td>English</td></tr>
</table>

II. INFORMATION ABOUT THE INSTRUCTOR

Name: Nazarii SHULIAK
Academic Title: PhD of 291 «International Relations, Public Communications and Regional Studies», senior lecturer of the International Relations Department
Contacts: 099 7783555, nazarii.shuliak@vnu.edu.ua
Days Classes: https://ps.vnu.edu.ua/cgi-bin/timetable.cgi

III. DESCRIPTION OF THE ELECTIVE ACADEMIC COMPONENT

1. *Course Abstract*

The elective academic component *Modern International Organizations in the Field of Information Security* is aimed at forming students’ understanding of the institutional architecture of global and regional information security and the role of international organizations in countering information threats, cyber risks, disinformation, and hybrid challenges. The course examines the mandates, structures, instruments, and practical activities of key international organizations operating in the field of information and cyber security, including the UN, NATO, EU, OSCE, Council of Europe, and specialized international agencies.

Special attention is paid to international legal frameworks, strategic documents, coordination mechanisms, and best practices of international cooperation in ensuring information resilience, cyber stability, and protection of democratic processes.

2. *Goal* of the course is to provide students with theoretical knowledge and analytical skills necessary to understand and assess the activities of modern international organizations in the field of information security. The main objectives are: to introduce the concept of information security in international relations; to

analyse the role of international organizations in global information governance; to study institutional mechanisms of countering cyber threats and disinformation; to assess international strategies, doctrines, and policy documents; to develop analytical skills in evaluating organizational effectiveness.

3. *Soft Skills: a*nalytical thinking; critical evaluation of information; strategic vision; institutional analysis; communication skills; teamwork; policy analysis; ethical reasoning; adaptability to security challenges; intercultural competence.

4. *Structure of the Elective Academic Component*

Names of Content Modules and Topics	**Total**	**Lectur.**	**Sem.**	**Cons.**	**Indep. work**	**Control/ Points***
Content module 1. International Information Security Architecture						
Topic 1. Information Security in International Relations: Concepts and Evolution	22	2	4	2	20	DS, P 20
Topic 2. Global Information Threats and Challenges	18	2	4	2	20	DS, P 20
Topic 3. International Legal Frameworks of Information Security	20	2	4	2	22	DS, P 20
Total for Content Module 1	**60**	**6**	**12**	**6**	**62**	**60**
Content Module 2. International and Regional Organizations in Practice						
Topic 4. NATO and Information Security Policies	27	2	4	2	24	DS, P 20
Topic 5. European Union and Digital Security Governance	33	2	4	2	24	DS, P 20
Total for Content Module 2	**60**	**4**	**8**	**4**	**48**	**40**
Total:	**120**	**10**	**20**	**10**	**110**	**100**

**Control methods: DS – discussion, DB – debate, T – tests, TR – training, PM/CM – problems/cases management, IST/ISW – individual task/individual work of the student, SGW – work in small groups, MTP/TP – module test paper/test paper, Ab – abstract, analytical note, analytical essay, analysis of the work, P – presentation.*

IV. TASKS FOR INDEPENDENT WORK

Independent work includes studying the material covered in practical classes. Students can work with the materials covered in practical classes on the distance learning platform https://teams.cloud.microsoft/. The effectiveness of independent work is assessed during thematic testing and reflected in the overall assessment of the elective academic component.

Tasks		Hours
Policy Document Analysis, Analytical Essays	- analytical essay «Information security in the system of modern international relations» (1500–2000 words); - identify key global threats: cyberwarfare, disinformation, hybrid operations; - create a timeline of major international initiatives and agreements. Prepare a short analytical summary.	20
Comparative Tables	– prepare a conceptual diagram: levels of information security (global–regional–national); – compare the mandates of key organizations in information and communication security; prepare a comparative table: functions, tools, influence, challenges.	20
Case Studies	-study UN initiatives in cybersecurity and information security; prepare a report: UN mechanisms for cyber stability; - study EU cybersecurity strategies and institutions; analyze the role of ENISA and CERT-EU; prepare a structured overview of EU cybersecurity governance; - analyze NATO cyber defense initiatives; Prepare a case analysis: NATO response to cyber incidents.	25
Reflection Papers	Reflection paper: Trust as a key factor in international cybersecurity cooperation	25
Research Projects	- analyze one strategic document (EU, NATO, UN). Prepare an analytical summary with key priorities and risks.	20
	Total	**110**

V. ASSESSMENT POLICY

The instructor's policy regarding the student. Attendance at classes is mandatory. For objective reasons (for example, illness, international internship, participation in scientific events, etc.), training may take place according to an individual plan in agreement with the instructor. In conditions of martial law or quarantine restrictions, the educational process at the university may be carried out in a mixed form of learning, namely: in person in the classroom or remotely in Microsoft Teams.

Academic Integrity Policy. Plagiarism, data falsification, and unauthorized use of AI tools are prohibited. If AI tools are used, students must clearly indicate this and bear responsibility for the validity and interpretation of results.

Deadlines and Rescheduling Policy. All theoretical tasks are submitted on the day of the seminar. Working students coordinate the assignment schedule with the instructor. Missed classes are passed only if there is confirmation of a valid reason

for the absence (certificate of absence due to illness or a statement about the need to miss classes).

If the student has completed the training and received the relevant Certificate, then the topic/topics of the discipline or modular test papers (work) can be counted (depends on the subject of the training and is decided separately in each individual case).

Opportunity to get additional (bonus) points. There is the respective system of bonuses at the International Relations Faculty and students may be added no more than 15 points to their current control.

VI. FINAL CONTROL

The credit is given based on the results of the current work, provided that the student has completed the types of academic work specified in the syllabus. If the student did not attend individual classroom classes, during consultations he/she has the right to work through the missed classes and get the number of points that was determined for the missed topics. On the date of the credit, the instructor writes down in the statement the amount of current points that the student scored during the current work (scale from 0 to 100 points). If the student scored less than 60 points during the current work, he/she takes the credit during the liquidation of academic debt. In this case, the points scored during the current assessment are cancelled. The maximum number of points for the credit during the liquidation of academic debt is 100.

Questions:

1. Information security as a field of international relations.
2. Global information threats and risks.
3. Role of the United Nations in information security.
4. International legal regulation of cyberspace.
5. NATO information and cyber security strategies.
6. EU digital and information security policies.
7. OSCE confidence-building measures.
8. Council of Europe standards in information security.
9. International cooperation against disinformation.
10. Cyber diplomacy and global governance.
11. Protection of democratic processes.
12. Information security and hybrid warfare.
13. Institutional effectiveness of international organizations.
14. Future trends in global information security.

VII. GRADING SCALE

Scores	Linguistic Grade
90-100	Passed
82-89	
75-81	
67-74	
60-66	
1-59	Fail (needed to retake)

VIII. REFERENCES

1. Шуляк Н. О., Шуляк А. М. Інформаційна гігієна в еру цифрових загроз: від пропаганди до гібридних атак. Серія: Історія. *Політологія*. 40. 2024. С. 185-195. DOI: 10.34079/2226-2830-2024-15-40-185-195.
2. Turner S., Tanczer L. M. In principle vs in practice: User, expert and policymaker attitudes towards the right to data portability in the internet of things DOI: 10.1016/j.clsr.2023.105912. URL: https://www.sciencedirect.com/science/article/pii/S026736492300122X.
3. Коротков Д. С. Міжнародні неурядові організації: характер впливу на сучасні міжнародні відносини. 2022. URL: https://repository.hneu.edu.ua/handle/123456789/28604.
4. Кононенко В. П., Новікова Л. В., Копицька П. О. Політика міжнародних організацій з питань інформаційної безпеки. *Науковий вісник Ужгородського національного університету.* Серія: Право. 65. 2021. С. 353-358. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/242834.
5. Смотрич Д. В., Браілко Л. Інформаційна безпека в умовах воєнного стану. 2023. URL: http://library.megu.edu.ua:8180/jspui/bitstream/123456789/4280/1/2023.pdf.
6. Шопіна І. М. Інформаційна безпека цифрової трансформації. *Науковий вісник Львівського державного університету внутрішніх справ* (серія юридична). (1). 2023. С. 28-35. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/5636.
7. Залєвська І. І., Удренас Г. І. Інформаційна безпека України в умовах російської військової агресії. 2022. URL: https://web.archive.org/web/20220820225319id_/http://www.sulj.oduvs.od.ua/archive/2022/1-2/6.pdf.
8. Центр стратегічних комунікацій та інформаційної безпеки. Гібридні загрози та комунікаційна безпека України. Аналітичні доповіді, 2022–2025. https://spravdi.gov.ua/

9. Національний інститут стратегічних досліджень (НІСД). Гібридна війна Росії проти України: інформаційний вимір. Київ, 2021–2024. URL: https://niss.gov.ua/.

10. Детектор медіа. Інформаційні операції та стратегічні наративи РФ. 2021–2024. URL: https://detector.media/.

11. StopFake. Дезінформація як інструмент гібридної війни. 2021–2024. URL: https://www.stopfake.org/.

12. NATO Strategic Communications Centre of Excellence. Hybrid Threats: A Strategic Communications Perspective. Riga, 2022. URL: https://stratcomcoe.org/.