Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Department of Management
Theory and Practice, FSP

OSINT TECHNOLOGIES IN SOCIOLOGICAL RESEARCH

Curriculum (Syllabus)

Course details

Level of higher education	***Second (Master's)***
Field of knowledge	*C - social sciences, journalism, information and international relations*
Specialisation	*C5 Sociology*
Educational programme	*Social Data Analytics*
Status of discipline	*Mandatory*
Form of study	*Full-time (day)*
Year of study, semester	*2nd year, autumn semester*
Scope of the discipline	*4 credits / 120 hours* *16 hours of lectures, 30 hours of practical classes, 74 hours of independent work.*
Semester assessment/assessment measures	*Test / modular control work*
Class schedule	*https://schedule.kpi.ua/*
Language of instruction	*Ukrainian*
Information about course director / lecturers	Lecturer: *Ilya Varzhansky* Practical / Seminar: *Lecturer Ilya Varzhansky*
Course location	*A link to the distance learning resource will be provided during the first class*

Course programme

1. Description of the course, its purpose, subject matter and learning outcomes

The course "OSINT Technologies in Sociological Research" is aimed at studying methods of collecting, analysing and interpreting open sources of information for conducting research and making decisions in the social sciences. OSINT (Open Source Intelligence) is a critical tool for analysing data available from open sources such as the media, social networks, public databases, official reports, etc.

The aim of the course *is to teach students methods for the effective use of open data to obtain useful information and develop critical analysis skills using modern digital technologies, as well as to provide students with the knowledge, skills and abilities necessary to work with open sources of information in the context of sociological research and analytics. Students will learn how to effectively use tools for collecting, processing, and analysing data from open sources, which will contribute to their professional development in the field of social sciences and media analysis.*

Subject *of* ***the academic discipline.*** *The course combines theoretical and practical aspects, allowing students to learn how to use modern tools for collecting, processing and analysing data from open sources.*

Competencies acquired during the course:

1. ***General competence:***
    - *GC 01. Ability to think abstractly, analyse and synthesise.*
2. ***Professional (subject) competencies:***
    - *PC 01. Ability to analyse social phenomena and processes.*
    - *PC 04. Ability to collect and analyse empirical data using modern methods of sociological research.*
    - *PC 11. Ability to analyse open source intelligence (OSINT), analyse qualitative information and textual data, and use intellectual analysis for social data.*

Programme learning outcomes:

- *PRN 01. Analyse social phenomena and processes using empirical data and modern concepts and theories of sociology.*
- *PRN 04. Apply scientific knowledge, sociological and statistical methods, digital technologies, and specialised software to solve complex problems in sociology and related fields of knowledge.*
- *PRN 05. Search for, analyse and evaluate necessary information in scientific literature, databases and other sources.*
- *PRN 12. Analyse open source intelligence (OSINT), analyse qualitative information and text data, and use intelligent analysis for social data.*

2. Prerequisites and post-requisites of the discipline (place in the structural-logical scheme of training under the relevant educational programme)

Prerequisites. *To successfully study the discipline "OSINT Technologies in Sociological Research", students must have knowledge and skills in the following disciplines:*

1. ***R and Python programming languages in statistical computing*** *– provides the technical programming skills necessary for working with data in open sources.*

At the same time, "OSINT Technologies in Sociological Research" is studied with the following educational components:

1. ***Big data analysis and artificial intelligence*** *– allows for deeper development of skills in working with large data sets that can be collected from open sources.*
2. ***Research work on the topic of the master's thesis*** *– the skills and knowledge gained from OSINT can be used when conducting research for the master's thesis.*

Post-requisites. *After completing the course "OSINT Technologies in Sociological Research," students will be able to continue their studies or perform research tasks within the educational component:*

3. ***Master's thesis*** *– application of OSINT research results for forecasting and modelling social processes, conducting analytics, etc.*

These disciplines form a logical sequence of learning that contributes to the development of analytical and research competencies of students.

3. Contents of the academic discipline

Topic 1: Introduction to OSINT

- *Definition of OSINT.*
- *History and development of OSINT.*
- *Ethical and legal aspects of OSINT.*

- *Overview of the main sources of information.*
- ***Practical exercise:*** *Introduction to basic OSINT tools, searching for information about a public figure.*

Topic 2: OSINT methods and tools

- *Methodology for conducting OSINT research.*
- *Overview of popular OSINT tools.*
- *Techniques for verifying information.*
- ***Practical work:*** *Working with tools for verifying legal entities, analysing the organisation's tenders.*

Topic 3: OSINT in cybersecurity

- *The role of OSINT in cybersecurity.*
- *Methods for identifying vulnerabilities using OSINT.*
- ***Practice:*** *Working with tools for analysing domains and IP addresses, researching potential threats to a given organisation.*

Topic 4: Geolocation and visual OSINT

- *Methods for determining location using open data.*
- *Image and video analysis in OSINT.*
- *Using satellite images and maps.*
- ***Practical*** *work****:*** *Working with geolocation and image analysis tools, determining location from a photograph.*

Topic 5: Advanced OSINT techniques

- *Advanced OSINT methods (DARKINT, CROSINT).*
- *Automation of OSINT processes.*
- *The future of OSINT and new trends.*
- ***Practical work:*** *Demonstration of automated OSINT tools, investigation in the Telegram messenger.*

Topic 6: Social media as a source of OSINT

- *Types of data in social media.*
- *Tools for collecting data from social media.*
- *Ethical aspects of collecting information on social networks.*
- ***Practical exercise:*** *Using social media analysis tools, creating a profile based on open data.*

Topic 7: Legal aspects and ethics of OSINT

- *International legal standards for the use of open data.*
- *Privacy and personal data protection in OSINT.*
- ***Practice:*** *Analysis of cases of privacy and human rights violations in OSINT operations.*

Topic 8: Using OSINT in investigations.

- *OSINT methods for investigations in journalism and law enforcement.*
- *Practical cases of OSINT use in international investigations.*
- ***Practice:*** *Conducting a mini-investigation using open sources.*

Topic 9: Verification of information and falsification of data

- *Methods for verifying the accuracy of information.*
- *Detecting data falsification and disinformation.*
- ***Practice:** Using tools to verify media data and recognise fake news.*

4. Training materials and resources

Basic literature:

1. *Lande D. V. OSINT in cybersecurity: textbook. Kyiv: Engineering LLC, 2024. 522 p. URL: http://dwl.kiev.ua/art/OSINT/OSINT-DEMO.pdf (accessed: 16.06.2024).*
2. *Zorenko D. S., Lekh R. V., Kulik D. O., Chervyakov O. I. Using OSINT tools and methods to obtain search information: a practical guide / Institute for Training Legal Personnel for the Security Service of Ukraine. Kharkiv, 2023. 36 p. URL: https://dspace.nlu.edu.ua/bitstream/123456789/19712/1/P_OSINT.pdf (accessed on 16 June 2024).*
3. *Revak I., Pidkhomnyi O., Chubaievskyi V. Electronic documents as resources for sociological research on the level of security of financial and legal relations. Social and Legal Studies. 2024. Vol. 7, No. 1. P. 273-282. URL: https://doi.org/10.32518/sals1.2024.273 (accessed on 16 June 2024).*

Additional reading:

1. *Basic OSINT course from Molfar. OSINT community Molfar : website. URL: https://www.udemy.com/course/osint-molfar/ (accessed: 16.06.2024).*
2. *OSINT – what it is, essence, definition and examples, types, methods and tools of open source intelligence. Termin.in.ua: website. URL: https://termin.in.ua/osint-rozvidka-na-osnovi-vidkrytykh-dzherel/ (accessed on 16 June 2024).*
3. *Brovko L. OSINT technologies: how open sources help media professionals. Press Association UA : website. URL: https://pressassociation.org.ua/ua/tehnologi%D1%97-osint-yak-vidkriti-dzherela-dopomagayut-medijnikam/ (accessed: 16.06.2024)*
4. *DeGarmo A. The OSINT Codebook. Cracking open source intelligence strategies. 2022. 212 p. URL: https://dokumen.pub/the-osint-codebook-cracking-open-source-intelligence-strategies-9798223202868.html (date of access: 16.06.2024).*
5. *What is OSINT (Open-Source Intelligence?). SANS Institute. Cyber Security Training. URL: https://www.sans.org/blog/what-is-open-source-intelligence/ (date of access: 16.06.2024).*
6. *Ludo Block. The long history of OSINT. JOURNAL OF INTELLIGENCE HISTORY. 2024. Vol. 23, No. 2. Pp. 95–109. URL:*

   https://www.tandfonline.com/doi/epdf/10.1080/16161262.2023.2224091?needAccess=true (date of access: 16.06.2024).

Educational content

5. Methodology for mastering the academic discipline (educational component)

5.1 Lectures

1. ***Lecture 1: Introduction to OSINT***
   - ***Key questions:***
     - *Definition of OSINT.*
     - *History and development of OSINT.*

- *Ethical and legal aspects of OSINT.*
- *Overview of key sources of information.*

- ***Recommended reading:***
  - *Lande D. V. OSINT in cybersecurity: textbook. Kyiv: Engineering LLC, 2024. 522 p.*
  - *Ludo Block. The long history of OSINT. JOURNAL OF INTELLIGENCE HISTORY. 2024. Vol. 23, No. 2. P. 95–109.*

2. ***Lecture 2: OSINT methods and tools***
   - ***Key questions:***
     - *Methodology for conducting OSINT research.*
     - *Overview of popular OSINT tools.*
     - *Techniques for verifying information.*
   - ***Recommended reading:***
     - *Lande D. V. OSINT in cybersecurity: textbook. Kyiv: Engineering LLC, 2024. 522 p.*
     - *DeGarmo A. The OSINT Codebook. Cracking open source intelligence strategies. 2022. 212 p.*
3. ***Lecture 3: OSINT in cybersecurity***
   - ***Key questions:***
     - *The role of OSINT in cybersecurity.*
     - *Methods for detecting vulnerabilities using OSINT.*
   - ***Recommended reading:***
     - *Lande D. V. OSINT in cybersecurity: textbook. Kyiv: Engineering LLC, 2024. 522 p.*
     - *Zorenko D. S., Lekh R. V., Kulik D. O., Chervyakov O. I. Using OSINT Tools and Methods to Obtain Search Information: A Practical Guide / Institute for Training Legal Personnel for the Security Service of Ukraine. Kharkiv, 2023. 36 p.*
4. ***Lecture 4: Geolocation and visual OSINT***
   - ***Key questions:***
     - *Methods for determining location using open data.*
     - *Analysis of images and videos in OSINT.*
     - *Use of satellite images and maps.*
   - ***Recommended reading:***
     - *Lande D. V. OSINT in cybersecurity: textbook. Kyiv: Engineering LLC, 2024. 522 p.*
     - *DeGarmo A. The OSINT Codebook. Cracking open source intelligence strategies. 2022. 212 p.*
5. ***Lecture 5: Advanced OSINT techniques***
   - ***Key questions:***
     - *Advanced OSINT methods (DARKINT, CROSINT).*
     - *Automation of OSINT processes.*
     - *The future of OSINT and new trends.*

- ***Recommended reading:***
  - *Lande D. V. OSINT in cybersecurity: textbook. Kyiv: Engineering LLC, 2024. 522 p.*
  - *DeGarmo A. The OSINT Codebook. Cracking open source intelligence strategies. 2022. 212 p.*

6. ***Lecture 6: Social media as a source of OSINT***
   - ***Key questions:***
     - *Types of data in social media.*
     - *Tools for collecting data from social media.*
     - *Ethical aspects of collecting information on social networks.*
   - ***Recommended reading:***
     - *Lande D. V. OSINT in cybersecurity: textbook. Kyiv: Engineering LLC, 2024. 522 p.*
     - *Brovko L. OSINT technologies: how open sources help media professionals. Press Association UA: website.*
7. ***Lecture 7: Legal aspects and ethics of OSINT***
   - ***Key questions:***
     - *International legal standards for the use of open data.*
     - *Privacy and personal data protection in OSINT.*
   - ***Recommended reading:***
     - *Lande D. V. OSINT in cybersecurity: textbook. Kyiv: Engineering LLC, 2024. 522 p.*
     - *Zorenko D. S., Lekh R. V., Kulik D. O., Chervyakov O. I. Use of OSINT tools and methods for obtaining search information: practical guide / Institute for Training Legal Personnel for the Security Service of Ukraine. Kharkiv, 2023. 36 p.*
8. ***Lecture 8: Using OSINT in investigations. Verification of information and falsification of data***
   - ***Key questions:***
     - *OSINT methods for investigations in journalism and law enforcement.*
     - *Practical cases of OSINT use in international investigations.*
     - *Methods for verifying the accuracy of information.*
     - *Detection of data falsification and disinformation.*
   - ***Recommended reading:***
     - *Lande D. V. OSINT in cybersecurity: textbook. Kyiv: Engineering LLC, 2024. 522 p.*
     - *Zorenko D. S., Lekh R. V., Kulik D. O., Chervyakov O. I. Use of OSINT tools and methods for obtaining search information: practical guide / Institute for Training Legal Personnel for the Security Service of Ukraine. Kharkiv, 2023. 36 p.*

5.2 Seminar classes

1. ***Seminar 1-2: Introduction to OSINT***
   - *Analysis of information sources.*
   - *Practical task: Searching for information about a public figure.*

2. ***Seminar 3-4: OSINT methods and tools***
    - *Working with tools for verifying legal entities.*
    - *Practical task: Analysis of the organisation's tenders.*
3. ***Seminar 5-6: OSINT in cybersecurity***
    - *Working with tools for analysing domains and IP addresses.*
    - *Practical task: Researching potential threats to a given organisation.*
4. ***Seminar 7-8: Geolocation and visual OSINT***
    - *Working with geolocation and image analysis tools.*
    - *Practical task: Determining location from a photograph.*
5. ***Workshop 9-10: Advanced OSINT techniques***
    - *Demonstration of automated OSINT tools.*
    - *Practical task: Investigation in the Telegram messenger.*
6. ***Workshop 11: Social media as a source of OSINT***
    - *Using social media analysis tools.*
    - *Practical task: Creating a profile of a person based on open data.*
7. ***Workshop 12: Legal aspects and ethics of OSINT***
    - *Analysis of cases of privacy and human rights violations in OSINT operations.*
8. ***Workshop 13: Using OSINT in investigations***
    - *Conducting a mini-investigation using open sources.*
9. ***Workshop 14: Verification of information and data falsification***
    - *Using tools to verify media data.*
    - *Practical task: Recognising fake news.*
10. ***Seminar 15:*** *Modular control work*

Teaching methods and technologies*. Didactic methods, observation and comparison, generalisation and abstraction, analogy, induction, deduction, analysis and synthesis, analytical-synthetic, abstract-deductive, concrete-inductive, explanatory-illustrative, reproductive, partial-search, research. Also, a set of methods, including practical, visual, verbal, problem-solving, partial-search, and other groups of methods. Among the teaching methods, analytical, inductive, deductive, and tradutive methods are used according to the nature of cognitive logic.*

Multimedia equipment and computers are used in classes. Distance learning uses Zoom and/or Google Meet video conferencing services, the Google Classroom educational web service on the Sikorsky platform, messengers for communication with students, and the university software of the Electronic Campus information and communication system.

6. Independent work of higher education students

Independent work by students is an important part of the learning process and involves completing a series of tasks that promote deeper understanding of the course material and the development of practical skills in OSINT research.

Types of independent work:

1. ***Preparation for classroom sessions (seminars):***
    - *Students should prepare for seminars by studying the recommended materials and literature, as well as searching for information on the given topic from open sources.*

- *Approximate time: 2 hours to prepare for each seminar (28 hours in total).*

2. ***Searching for and analysing information from open sources:***
   - *Searching for information using OSINT tools (e.g., searching for information about a public figure or organisation, analysing tenders, checking IP addresses, etc.).*
   - *Approximate time: 10 hours for the practical application of OSINT tools as part of the course assignment.*
3. ***Completing individual practical assignments:***
   - *Completing practical tasks related to lecture topics, such as conducting research using geolocation or image analysis.*
   - *Approximate time: 16 hours during the semester.*
4. ***Writing an essay or preparing an analytical report:***
   - *Writing a report or analytical report based on OSINT research on a specific topic.*
   - *Approximate time: 10 hours.*
5. ***Preparation for the modular control work and final exam:***
   - *Students must independently prepare for the modular control work and final semester exam by reviewing lecture material, completing additional assignments using OSINT tools, and studying the recommended literature.*
   - *Approximate time: 10 hours.*

Total time allocated for independent work: 74 hours.

Independent work must be properly organised and planned by students to ensure effective mastery of the subject and successful completion of all tasks.

Policy and control

7. Policy of the academic discipline (educational component)

Class attendance:

- *Attendance at lectures is optional but recommended, as lecture materials are an important component for understanding practical tasks and successfully passing the exam.*
- *Participation in seminars is mandatory, as they involve practical tasks and discussions that are important for developing the necessary competencies.*
- *Students who have missed classes for valid reasons have the opportunity to make up for the missed material during consultations with the teacher or by completing additional assignments.*

Class participation:

- *Students are encouraged to actively participate in seminar discussions and to prepare short reports and presentations based on their research.*
- *The use of electronic devices during classes is permitted exclusively for educational purposes (searching for information, participating in discussions via electronic platforms).*

Academic integrity:

- *Students must adhere to the principles of academic integrity, in particular avoiding plagiarism, falsification of data, and unauthorised use of other people's materials.*

- *Any violation of academic integrity (plagiarism, cheating, falsification of results) will result in a negative grade for the assignment and may affect the final grade.*

Recognition of informal education results:

- *Students have the opportunity to transfer credits from online courses or other forms of informal education on topics relevant to the content of the discipline, subject to agreement with the lecturer and provision of the relevant certificate.*

Deadline and retake policy:

- *All assignments must be submitted on time. Students are allowed to retake a modular control work or exam in case of an unsatisfactory result, but no more than twice.*

8. Types of assessment and the learning outcomes assessment rating system (LOAS)

Types of assessment and evaluation:

Student knowledge will be assessed on the basis of ongoing assessment, modular control work and a final test. The maximum number of points for the course is 100.

1. ***Ongoing assessment (70 points, 5 points for 14 practical (seminar) classes):***
    - ***Work in a seminar class (up to 5 points):*** *The student's activity during discussions, preparation of reports and co-reports, and completion of practical tasks will be assessed.*
        - *5 points — active participation in all classes and high-quality performance of tasks.*
        - *4-3 points — partial participation in classes or average performance of tasks.*
        - *1-2 points — low activity or poor performance of tasks.*
        - *0 points — missed seminar classes without make-up work.*
    - ***Modular control work (30 points):*** *Conducted at the end of the course after studying the main topics. Consists of two parts: theoretical (open questions) and practical (completion of tasks using OSINT tools).*
        - *28-30 points — complete and correct answers to all tasks.*
        - *23-27 points — generally correct answers, minor inaccuracies or isolated errors that do not affect the overall result.*
        - *18-22 points - partial errors or imperfect completion of tasks.*
        - *0-17 points - incorrect or incomplete answers.*

Calendar control. *Calendar certification of higher education applicants (hereinafter referred to as certification) is conducted twice per semester as monitoring of the current status of fulfilment of the Syllabus requirements. The purpose of certification is to improve the quality of education of higher education applicants and to monitor the implementation of the educational process schedule. For the first assessment, the student must score at least 15 points for the current control, for the second - at least 30 points.*

Conditions for admission to the exam:

- *To be admitted to the exam, a student must score at least 30 points for current control and modular control work.*

Additional points:

- *Students can earn up to 10 additional points for active participation in international or national events related to the course topic, publication of scientific articles, participation in OSINT and data analytics projects.*

Conducting the exam:

Students who have scored 60 or more points during the semester have the opportunity to:

- *receive a credit grade (credit) according to the rating obtained (rating points are converted to a grade according to the table and entered into the semester control record);*
- *take a credit test in order to improve their grade (in this case, the student's previous rating in the discipline is cancelled and they receive a grade based solely on the results of the credit test).*

Students who have scored less than 60 points during the semester but have fulfilled the admission requirements take a credit test.

Answers to the test are assessed on a scale of 100 points and are awarded for answers to 2 questions:
-complete answer/completed task (at least 90% of the required information) – 50-45 points;
-sufficiently complete answer/completed task (at least 75% of the required information) – 44-38 points;
-incomplete answer/completed task (at least 60% of the required information) – 37-30 points;
-incomplete answer/task not completed (less than 60% of the required information) – 29-0 points.

Table of correspondence between rating points and university scale grades:

Number of points	*Grade*
100-95	*Excellent*
94	*Very good*
84	*Good*
74-65	*Satisfactory*
64-60	*Sufficient*
Less than 60	*Unsatisfactory*
Admission requirements not met	*Not admitted*

9. Additional information on the discipline (educational component)

List of questions for the test:

1. *Define OSINT and describe its basic principles.*
2. *What are the main sources of information used in OSINT research?*
3. *Describe the history of OSINT development and its significance in the modern world.*
4. *What legal and ethical aspects need to be considered when conducting OSINT research?*
5. *How is data verification carried out in OSINT? Describe the main techniques for verifying information.*
6. *Name popular OSINT tools and describe their functions.*
7. *How is OSINT used in cybersecurity? Give examples.*
8. *Describe methods for detecting cyber threats using OSINT.*
9. *How are domains and IP addresses analysed in the context of OSINT research?*
10. *What is geolocation in the context of OSINT and how is it used for analysis?*
11. *How are images and videos analysed in OSINT research?*
12. *What tools are used to analyse satellite images and maps?*
13. *Describe advanced OSINT methods (DARKINT, CROSINT) and their features.*
14. *What is process automation in OSINT and what tools are used for this?*
15. *What trends in the future development of OSINT can you identify?*
16. *What social media data can be used for OSINT research?*
17. *How do tools for collecting data from social media work?*
18. *What ethical aspects need to be considered when collecting data from social networks?*
19. *Describe the international legal standards governing the use of OSINT.*
20. *What privacy and personal data protection aspects should be considered during OSINT research?*

21. *How is OSINT used in journalistic investigations? Give examples.*
22. *Describe the role of OSINT in law enforcement investigations.*
23. *Describe the process of conducting OSINT research using social networks.*
24. *What methods are used to verify information obtained through OSINT?*
25. *How can you detect falsified data and disinformation using OSINT?*
26. *What techniques are used to verify the authenticity of images and videos?*
27. *Describe how investigations are conducted in messengers based on open sources.*
28. *How is the analysis of legal entities conducted using OSINT?*
29. *What tools are used to analyse tenders and contracts in OSINT?*
30. *What approaches are used to collect and process large amounts of data in OSINT research?*

.

Work programme for the academic discipline (syllabus):

Compiled *by Ilya Varzhansky, lecturer at the Department of Management Theory and Practice*

Approved *by the Department of Management Theory and Practice (Minutes No. 15 of 19 June 2025)*

Approved by *the Methodological Commission of the Faculty of Sociology and Law (Minutes No. 4 of 24 June 2025)*