Силабус освітнього компоненту
«Соціальна інженерія та маніпулятивні практики в цифровому просторі»
Галузь знань: Соціальні науки, журналістика, інформація та міжнародні відносини
Спеціальність: *052 Політологія*
Освітня програма: Політологія (мова навчання – українська)
Рівень вищої освіти: перший (бакалаврський)
Рік навчання: 2027-2028
Семестр: денна форма – 7; **заочна форма** -7

Структурний підрозділ	Кафедра політології та філософії, історичний факультет
Викладач: 	**Прізвище, ім'я, по батькові:** Грубі Тетяна Вікторівна **Посада:** завідувач кафедри політології та філософії **Науковий ступінь:** кандидат соціологічних наук **Вчене звання:** доцент **E-mail:** biletsky.tatiana@kpnu.edu.ua **Робоче місце:** навчальний корпус №2 (вул. Татарська, 14), кафедра політології та філософії. **ORCID:** https://orcid.org/0000-0002-8844-5842 **Профайл викладача:** https://politkaf.kpnu.edu.ua/vinnichuk-olha-vasylivna/ https://scholar.google.com/citations?hl=uk&user=wpHz_KIAAAAJ https://www.webofscience.com/wos/author/record/HNS-2682-2023
Лінк на освітній контент дисципліни	https://moodle.kpnu.edu.ua/course/view.php?id=11080
Статус дисципліни	вибірковий освітній компонент професійної підготовки
Обсяг дисципліни, кредити ЄКТС / години	4 кредити ЄКТС / 120 год.
Мова викладання	Українська
Форми навчання	Денна, заочна.
Політика дисципліни	**Академічна доброчесність.** Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її не зарахування викладачем, незалежно від масштабів плагіату чи обману. URL: https://integrity.kpnu.edu.ua/ Використання здобувачами вищої освіти в освітньому процесі інструментів ШІ чітко визначено "Положенням про використання штучного інтелекту в Кам'янець-Подільському національному університеті імені Івана Огієнка", введено в дію наказом в.о. ректора від 02 вересня 2026 р., № 144-ОД. URL: https://drive.google.com/file/d/1eDvHgbvZUYojWNwNwkIED66qGDPPpHrB/view

Що будемо вивчати?	У межах навчальної дисципліни передбачено вивчення теоретико-методологічних засад соціальної інженерії та маніпулятивних практик у цифровому комунікаційному середовищі. Здобувачі освіти опановуватимуть аналіз когнітивно-психологічних механізмів і детермінант маніпулятивного впливу на особистість, а також технологій та методів отримання конфіденційної інформації (фішинг, претекстинг, вішинг). Окрема увага приділятиметься дослідженню стратегій впливу в соціальних мережах (ботоферми, астротурфінг, інформаційні «бульбашки»), феномену дезінформації та пропаганди (фейк-ньюз, дипфейк-технології), а також формуванню практичних навичок медіакомпетентності, критичного мислення та цифрової резильєнтності як базових компонентів інформаційно-психологічної безпеки.
Чому це треба вивчати?	Актуальність вивчення курсу зумовлена стрімким зростанням інформаційно-психологічних загроз у сучасному цифровому просторі та об'єктивною потребою суспільства у фахівцях, здатних ефективно протидіяти деструктивним впливам. Для майбутніх психологів опанування цієї дисципліни є професійно необхідним, оскільки дозволяє сформувати здатність до ідентифікації ознак маніпулятивної поведінки, розуміння природи кібербулінгу та надання кваліфікованої психологічної допомоги особам, які зазнали негативного інформаційного впливу.
Яких результатів можна досягнути?	Опанування навчальної дисципліни забезпечує формування цілісної системи теоретичних знань та практичних навичок, необхідних для аналізу й протидії деструктивним інформаційно-психологічним впливам у цифровому просторі. Зокрема, здобувачі вищої освіти досягнуть таких результатів: – розуміння теоретичних засад соціальної інженерії; знання когнітивно-психологічних механізмів маніпулятивного впливу на особистість; обізнаність із типологією та алгоритмами реалізації технік соціальної інженерії (фішинг, претекстинг, вішинг); розуміння принципів функціонування дезінформації, пропаганди, ботоферм та дипфейк-технологій у соціальних мережах. – вміння ідентифікувати та диференціювати прояви маніпулятивної комунікації та фейкові інформаційні приводи; застосовувати інструменти фактчекінгу та критичного аналізу медіатекстів; визначати психологічні вразливості особистості, що можуть бути використані зловмисниками в цифровому середовищі; аналізувати соціально-психологічні наслідки інформаційних атак. – Оволодіння знаннями про методи цифрової гігієни та захисту персональних даних; розробка та впровадження стратегій інформаційно-психологічної резильєнтності особистості; здатність надавати первинну психологічну підтримку особам, які зазнали маніпулятивного впливу, кібербулінгу або стали жертвами шахрайства в мережі Інтернет.
Як можна використати набуті знання та уміння?	Набуті в межах навчальної дисципліни знання та вміння мають широкий спектр практичного застосування і можуть бути використані у таких напрямах: У політичній аналітиці та консалтингу вони дозволять ідентифікувати ознаки маніпулятивних стратегій у політичній рекламі, передвиборчих кампаніях і публічних дискурсах, здійснювати фактчекінг політичних заяв та оцінювати інформаційні ризики для політичних акторів. У сфері політичної комунікації та зв’язків з громадськістю набуті компетентності стануть у нагоді для розробки етичних і безпечних стратегій взаємодії з аудиторією, протидії дезінформації та формування медіаграмотної політичної культури. Окремо слід відзначити цінність цих знань для державного управління та місцевого самоврядування — вони допоможуть виявляти спроби зовнішнього або внутрішнього маніпулятивного впливу на інформаційний простір, розробляти заходи з інформаційної безпеки та підвищувати стійкість громад до деструктивних впливів. У громадсько-політичній діяльності (робота в партіях, громадських організаціях, аналітичних центрах) набуті вміння дозволять ефективно протидіяти ботофермам, астротурфінгу та фейковим наративам, а також будувати прозору комунікацію з виборцями. Крім того, вони сприятимуть особистій інформаційній безпеці політолога як публічного експерта та дозволять долучатися до розбудови національної системи інформаційної резильєнтності.

Зміст дисципліни	**Тема 1. Теоретико-методологічні засади соціальної інженерії в цифровому просторі.** Поняття, історія виникнення та еволюція соціальної інженерії. Визначення місця та ролі маніпулятивних практик у сучасному цифровому комунікаційному середовищі. **Тема 2. Психологічні механізми та когнітивні вразливості в цифровій комунікації.** Аналіз когнітивних викривлень, емоційних тригерів та соціально-психологічних механізмів, що використовуються для маніпулятивного впливу на особистість та соціальні групи. **Тема 3. Базові техніки соціальної інженерії (фішинг, претекстинг, вішинг).** Класифікація, алгоритми реалізації та характерні ознаки основних методів отримання несанкціонованого доступу до інформації. Аналіз реальних кейсів кібершахрайства та їхніх політичних наслідків. **Тема 4. Маніпулятивні практики в соціальних мережах та месенджерах.** Діяльність ботоферм, астротурфінг, створення фейкових акаунтів та інформаційних «бульбашок». Вплив алгоритмів соціальних мереж на формування суспільної думки та політичних уподобань. **Тема 5. Дезінформація та пропаганда як інструменти політичного впливу.** Механізми створення та поширення фейк-ньюз, маніпуляція фото- та відеоконтентом (технології deepfake). Аналіз політичних наративів та їхнього впливу на електоральну поведінку. **Тема 6. Політичний мікротаргетинг та психографічне профілювання виборців.** Технології збору та аналізу цифрових слідів користувачів. Використання Big Data та штучного інтелекту для персоналізованого політичного впливу та сегментації електорату. **Тема 7. Соціальна інженерія у виборчих кампаніях та політичному консалтингу.** Застосування маніпулятивних практик під час виборчих перегонів (чорний PR, компромат, атаки на репутацію). Дослідження етичних меж політичної комунікації та професійної діяльності політолога. **Тема 8. Інформаційно-психологічні операції (ІПСО) та гібридні загрози.** Специфіка діяльності державних та недержавних акторів у проведенні ІПСО. Аналіз російських інформаційних кампаній проти України та механізмів їхньої реалізації в цифровому просторі. **Тема 9. Медіаграмотність та критичне мислення як інструменти протидії маніпуляціям.** Методологія фактчекінгу, верифікації джерел та аналізу медіатекстів. Формування навичок критичного сприйняття інформації в умовах інформаційного шуму. **Тема 10. Цифрова гігієна та інформаційна безпека політолога.** Практичні аспекти захисту персональних даних, налаштування приватності та запобігання цифровим атакам. Забезпечення особистої безпеки публічного експерта та аналітика в мережі. **Тема 11. Правові та етичні аспекти протидії деструктивним інформаційним впливам.** Законодавче регулювання кібербезпеки, захисту персональних даних та протидії дезінформації в Україні та світі. Етичні норми професійної діяльності політолога. **Тема 12. Формування інформаційної резильєнтності суспільства та держави.** Стратегії розбудови стійкості громад до інформаційно-психологічних атак. Роль державних інституцій, громадянського суспільства та політичних інститутів у забезпеченні національної безпеки.
Методи навчання	Словесні, наочні методи: лекція (лекція-презентація, проблемна лекція, лекція-бесіда, лекція-дискусія), розповідь, пояснення, бесіда, дискусія, диспут, мозкова атака, робота з першоджерелами, словниками, посібниками, дидактичними матеріалами та іншими джерелами інформації, робота з інтернетними публікаціями та матеріалами вебсайтів, робота за таблицями, створення й демонстрування презентацій.
Інформаційне	**Основні джерела:** 1. Бадер А. Політичний інжиніринг та маніпулятивні технології в політиці. Луганськ: Вид-во ДЗ «ЛНУ імені Тараса Шевченка», 2018. 145 с. 2. Воронова С., Стайкуца С. Соціальна інженерія: практикум для проактивних. Одеса: Астропринт, 2026. 180 с.

<table>
<tr><td></td><td>3. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання. Київ: Інститут проблем національної безпеки, 2009. 164 с.
4. Медіаосвіта та медіаграмотність: навчально-методичний посібник. Умань: Візаві, 2023. 123 с.
5. Мітнік К., Саймон В. Мистецтво обману: контроль над людським елементом безпеки. Київ: Видавничий дім «Києво-Могилянська академія», 2021. 384 с.
6. Політичні маніпуляції під час виборчого процесу як загроза політичної безпеки та реалізації влади народу. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Публічне управління та адміністрування. 2023. Т. 34 (73). № 3. С. 25–32.
7. Почепцов Г. Г. Віртуальні війни. Київ: Видавничий дім «Києво-Могилянська академія», 2021. 215 с.
8. Почепцов Г. Г. Токсичний інфопростір. Як зберегти ясність мислення і свободу дії. Київ: Віват, 2022. 384 с.
9. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.
10. Суіменко Є. І. Соціальна інженерія: експериментальний курс лекцій. Київ: Інститут соціології НАН України, 2011. 222 с.
11. Фактчек. Практичний посібник / команда проєкту «Без Брехні»; під керівництвом О. Гороховського. Київ: Національний проєкт з медіаграмотності «Фільтр», 2025. 156 с.
12. Хеднегі К. Мистецтво обману. Соціальна інженерія в шахрайських схемах. Київ: Альпіна Паблішер, 2023. 430 с.</td></tr>
<tr><td>Обсяг дисципліни (години) та види занять</td><td>Денна форма здобуття вищої освіти: лекційні заняття (28 год.), семінарські заняття (20 год.), самостійна робота (72 год.);
Заочна форма здобуття вищої освіти: лекційні заняття (02 год.), семінарські заняття (6 год.), самостійна робота (104 год.);</td></tr>
<tr><td>Система оцінювання результатів навчання</td><td>Основними методами контролю відповідно до критеріїв оцінювання знань здобувачів освіти та ефективності засвоєння ними курсу грунтується на таких формах участі студентів у освітньому процесі, які підлягають поточному контролю: виступ з основного питання на семінарському занятті, модульна контрольна, самостійна робота. Підсумковою оцінкою є залік. Розподіл балів, які отримують студенти
<table>
<tr><td colspan="3"></td><td rowspan="2">Екзамен</td><td rowspan="2">Сума балів</td></tr>
<tr><td>Аудиторна робота</td><td>Самостійна робота</td><td>МКР</td></tr>
<tr><td>25</td><td>10</td><td>25</td><td>40</td><td>100</td></tr>
</table></td></tr>
<tr><td>Критерії оцінювання знань, умінь, навичок студентів на навчальних заняттях</td><td>Оцінювання на семінарських заняттях відбувається за 12 бальною системою відповідно до критеріїв визначених «Положенням про рейтингову систему оцінювання навчальних досягнень здобувачів вищої освіти Кам’янець-Подільського національного університету імені Івана Огієнка». URL: https://drive.google.com/file/d/1ZbMN35h-7ZSJBBOVvL2bTCaLtRbcQA86/view</td></tr>
<tr><td>Поточний контроль</td><td>Усне опитування, письмовий контроль, виконання самостійної роботи, модульна контрольна робота</td></tr>
<tr><td>Підсумковий контроль</td><td>Залік</td></tr>
<tr><td>Локація</td><td>URL: https://kpnu.edu.ua/rozklad-zaniat/</td></tr>
</table>