Силабус освітнього компоненту
«Основи кібергігієни та цифрової безпеки в політичній сфері»
Галузь знань: Соціальні науки, журналістика, інформація та міжнародні відносини
Спеціальність: *052 Політологія*
Освітня програма: Політологія (мова навчання – українська)
Рівень вищої освіти: другий (магістерський)
Рік навчання: 2027-2028
Семестр: денна форма – 1; **заочна форма** -1

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?	Основи кібергігієни та безпечної роботи в цифровому середовищі публічного сектору: законодавство України з кібербезпеки й захисту персональних даних, правила безпечної роботи в Інтернеті, управління ризиками, а також розпізнавання соціальної інженерії, фішингу, шахрайства, дипфейків та ІПСО. Окремо будемо вивчати цифрову безпеку в політичній сфері: захист електронних виборів і е-демократії, протидію кібератакам і дезінформації, безпечну роботу з державними реєстрами та конфіденційними даними, цифрову стійкість, протидію гібридним загрозам і цифровому авторитаризму, а також стратегії протидії інформаційним атакам та інструменти моніторингу інформаційного поля.
Чому це треба вивчати?	Актуальність вивчення курсу зумовлена стрімким зростанням кіберзагроз, поширенням дезінформації, соціальної інженерії та гібридних впливів у цифровому просторі, а також об'єктивною потребою суспільства у фахівцях, здатних забезпечувати безпечну роботу з інформацією в публічній сфері. Для майбутніх політичних діячів, державних службовців і фахівців із публічних комунікацій опанування цієї дисципліни є професійно необхідним, оскільки дозволяє сформувати здатність ідентифікувати кіберзагрози й маніпулятивні впливи, забезпечувати захист персональних даних і конфіденційної інформації, протидіяти інформаційним атакам та ухвалювати обґрунтовані рішення в умовах цифрових ризиків.
Яких результатів можна досягнути?	Зокрема, здобувачі вищої освіти досягнуть таких результатів: розуміння теоретичних засад кібергігієни та цифрової безпеки; знання нормативно-правових основ кібербезпеки й захисту персональних даних в Україні; обізнаність із типологією та алгоритмами реалізації технік соціальної інженерії (фішинг, претекстинг, вішинг); розуміння принципів функціонування дезінформації, пропаганди, ботоферм, дипфейк-технологій та ІПСО в цифровому просторі; усвідомлення особливостей кіберзагроз у виборчих процесах, електронній демократії та роботі з державними реєстрами. Вміння ідентифікувати та диференціювати прояви кібератак, маніпулятивної комунікації та фейкові інформаційні приводи; застосовувати інструменти фактчекінгу, OSINT і критичного аналізу медіатекстів; визначати вразливості інформаційних систем і людського чинника, що можуть бути використані зловмисниками; аналізувати соціально-політичні наслідки інформаційних атак і кіберінцидентів. Оволодіння знаннями про методи цифрової гігієни та захисту персональних даних; розробка та впровадження стратегій цифрової стійкості політичних суб'єктів і публічних інституцій; здатність реагувати на кіберінциденти, складати плани дій в умовах інформаційної атаки та надавати рекомендації щодо безпечної роботи з конфіденційною інформацією в політичній діяльності.
Як можна використати набуті знання та уміння?	Набуті знання та уміння можна використати в аналітичній, консультативній, комунікаційній, виборчій та публічно-управлінській діяльності. Зокрема: – у політичному аналізі та прогнозуванні: оцінка інформаційних загроз, моніторинг дезінформації й ІПСО, виявлення ботоферм і дипфейків, підготовка аналітичних довідок і рекомендацій; – у консультуванні політичних суб'єктів: розробка політик цифрової безпеки для партій, депутатів, кандидатів і громадських організацій, навчання команд кібергігієни; – у виборчих кампаніях: забезпечення захисту акаунтів і комунікацій, протидія фейкам та атакам на репутацію, планування дій на випадок кіберінцидентів; – у публічному управлінні та місцевому самоврядуванні: безпечна робота з персональними даними й реєстрами, оцінка ризиків, підготовка внутрішніх інструкцій і чек-листів; – у громадському секторі та аналітичних центрах: фактчекінг, OSINT-дослідження, кампанії з медіаграмотності та цифрової стійкості; – у медіа й публічних комунікаціях: критичний аналіз медіатекстів, підготовка спростувань, комунікація під час інформаційних атак;

Зміст дисципліни	В межах курсу передбачено вивчення таких тем: **1. Цифровізація політики та концептуальні засади кібергігієни.** Вплив цифрових технологій на політичні процеси; поняття кібергігієни, цифрової безпеки й цифрової стійкості; роль людського чинника в політичних організаціях. **2. Державна політика у сфері кібербезпеки та захисту персональних даних.** Нормативно-правова база України, інституційна архітектура кібербезпеки, баланс між безпекою та правами людини. **3. Політична комунікація в цифровому середовищі та її вразливості.** Безпека акаунтів і каналів комунікації політичних суб'єктів; двофакторна автентифікація, захист пошти й месенджерів як складова політичної діяльності. **4. Соціальна інженерія як інструмент політичного впливу.** Фішинг, претекстинг, вішинг; психологічні механізми маніпуляції; аналіз кейсів атак на політиків, партії та держслужбовців. **5. Дезінформація, пропаганда та ІПСО в політичному процесі.** Ботоферми, дипфейки, маніпуляції суспільною думкою; фактчекінг, OSINT і критичний аналіз медіатекстів як інструменти політолога. **6. Кібербезпека виборчих процесів і електронної демократії.** Загрози виборчим системам і кампаніям; протидія атакам на репутацію; міжнародний досвід забезпечення виборчої кіберстійкості. **7. Цифрова безпека в публічному управлінні та роботі з реєстрами.** Захист конфіденційних даних, оцінка ризиків, внутрішні політики безпеки в органах влади та політичних організаціях. **8. Гібридні загрози, цифровий авторитаризм і масове спостереження.** Вплив цифрових технологій на демократичні інститути; маніпуляції суспільною думкою; захист демократії в умовах інформаційних війн. **9. Цифрова стійкість політичних суб'єктів і комунікація під час інцидентів.** Планування реагування на кібератаки та інформаційні кризи; роль політичного лідерства й комунікаційних стратегій. **10. Практикум політолога з цифрової безпеки.** Аналіз кейсів, симуляції (tabletop) кібератаки на виборчий процес та інформаційної атаки на політика, розробка чек-листів цифрової гігієни й стратегій протидії загрозам для політичних організацій.
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 наповнення	1. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. В. Б. Толубка. Київ: ДУТ, 2015. 288 с. 2. Вальорска М. А. Діпфейк та дезінформація: практ. посіб. / М. А. Вальорска ; пер. з нім. В. Олійника. Київ: Академія української преси ; Центр Вільної Преси, 2020. 36 с. 3. Завгородня Ю. В. Кіберзагрози в сучасному політичному просторі: метод. вказ. для підгот. до практич. занять та самост. роботи здобувачів вищої освіти другого (магістерського) рівня галузі знань – 05 «Соціальні та поведінкові науки», спец. 052 «Політологія» / Ю. В. Завгородня ; Нац. ун-т «Одеська юрид. академія». Одеса, 2024. 30 с. URL: https://hdl.handle.net/11300/28400. 4. Карпенко В. Інформаційна політика та безпека: підручник. Київ: Нора-Друк, 2016. 320 с. 5. Петрик В. М., Присяжнюк М. М., Мельник Д. С. та ін. Інформаційна безпека держави: підручник: у 2 т. / за заг. ред. В. М. Петрика. Київ: ДНУ «Книжкова палата України», 2016. Т. 1. 264 с.. 6. Ситник Г. П., Заворітня Г. П., Марутян Р. Р. Інформаційно-комунікаційні технології у сфері національної безпеки: навч. посіб. / за заг. ред. Г. П. Ситника. Київ: Академпрес, 2024. 175 с. 7. Shackelford S. J., Douzet F. (eds.). Securing Democracies: Defending Against Cyber Attacks and Disinformation in the Digital Age. Cambridge: Cambridge University

<table>
<tr><td></td><td>Press, 2026. 412 p.</td></tr>
<tr><td>Обсяг дисципліни (години) та види занять</td><td>Денна форма здобуття вищої освіти: лекційні заняття (20 год.), семінарські заняття (20 год.), самостійна робота (80 год.);

Заочна форма здобуття вищої освіти: лекційні заняття (8 год.), семінарські заняття (4 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 ґрунтується 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>