СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ПРОТИДІЯ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ В СУЧАСНИХ УМОВАХ ДЕРЖАВОТВОРЕННЯ»

Ступінь освіти	Бакалавр
Спеціальність	281 Публічне управління та адміністрування
Освітня програма	Публічне управління та адміністрування
Тривалість викладання	8-й семестр, 15 чверть
Кількість кредитів	4 кредити ЄКТС (120 годин)
Заняття:	
лекції:	1 година на тиждень
практичні:	2 години на тиждень
Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»

Кафедра, що викладає **Державного управління і місцевого самоврядування**

Консультації: за окремим розкладом, погодженим зі здобувачами вищої освіти

Онлайн-консультації: Terkhanov.F.I@nmu.one

Викладач:
Терханов Федір Іванович
к.держ.упр, доцент, доцент кафедри

E-mail:

Terkhanov.F.I@nmu.one

1. Анотація до курсу

Дисципліна присвячена вивченню теоретичних основ, механізмів, інструментів та практик забезпечення інформаційної безпеки особи, суспільства й держави в умовах сучасного інформаційного середовища. Курс охоплює ключові категорії інформаційних, інформаційно-психологічних та інформаційно-технічних загроз, розкриває сутність маніпулятивних технологій, принципи їх використання та моделі протидії деструктивним інформаційним впливам.

Особлива увага приділяється аналізу інформаційного протиборства як складової гібридних загроз, включно з інформаційною війною, інформаційним тероризмом, кіберзлочинністю та інструментами формування суспільної думки. Розглядаються загрози інформаційній безпеці України у політичній, соціальній, воєнній, економічній та гуманітарній сферах, а також методи їх ідентифікації та нейтралізації.

Навчальна дисципліна формує у здобувачів здатність ідентифікувати різні види інформаційних загроз, оцінювати рівень вразливості інформаційної інфраструктури, розуміти психологічні механізми впливу на свідомість і поведінку людини, розробляти стратегії інформаційної протидії та приймати обґрунтовані рішення у сфері інформаційної безпеки. Дисципліна інтегрує міждисциплінарні підходи — психологічні, комунікаційні, кібербезпекові, управлінські та правові.

Курс призначений для підготовки фахівців з державного управління, національної безпеки, стратегічних комунікацій, публічного управління, соціальних та поведінкових наук, комунікацій і кібербезпеки, забезпечуючи формування компетентностей, необхідних для професійної діяльності в умовах зростаючих інформаційних загроз.

2. Мета та завдання курсу

Метою навчальної дисципліни «Протидія інформаційним загрозам в сучасних умовах державотворення» є формування у здобувачів системного розуміння сутності, механізмів, форм і наслідків інформаційних, інформаційно-психологічних та інформаційно-технічних загроз, а також набуття компетентностей з ідентифікації інформаційних загроз, оцінювання їх впливу на особу, суспільство і державу та розроблення стратегій ефективної протидії в умовах сучасного інформаційного середовища.

Завдання курсу:

– ознайомити здобувачів вищої освіти із сутністю інформаційних, інформаційно-психологічних та інформаційно-технічних загроз, їх принципами, функціями та основними типами;

– розкрити тенденції еволюціонування інформаційних загроз як соціального, комунікаційного та безпекового явища, а також основні концепції інформаційного протиборства, інформаційної війни та гібридних загроз;

– визначити принципи забезпечення інформаційної безпеки, моделі управління інформаційними процесами, форми ефективної комунікації та механізми розвитку інформаційної стійкості особистості, соціальних груп і державних інституцій;

– розширити та систематизувати уявлення про класифікацію методів інформаційно-психологічних загроз, їх чинники, умови ефективності, а також психологічні, соціальні та технологічні передумови їхнього здійснення;

– ознайомити з інструментами протидії інформаційним загрозам, розкрити особливості формування та розвитку спроможностей інформаційної безпеки, механізмів захисту інформаційних ресурсів та стійкості інформаційної інфраструктури в соціальній сфері та державному управлінні;

– сформувати практичні навички критичного мислення, аналітичного оцінювання інформації, ідентифікації маніпулятивних впливів, аргументації та узагальнення висновків, а також здатність творчо генерувати нові ідеї для підвищення інформаційної безпеки та ефективної комунікації.

3. Результати навчання

Дисциплінарні результати навчання:

– продемонструвати знання: сутності інформаційних, інформаційно-психологічних та інформаційно-технічних загроз; принципів і функцій інформаційної безпеки; основних концепцій інформаційного протиборства, інформаційної війни, інформаційного тероризму та комп'ютерної злочинності; класифікації методів маніпулятивного впливу, умов їх ефективності та передумов застосування; базових механізмів забезпечення інформаційної безпеки особи, суспільства та держави;

– продемонструвати розуміння особливостей деструктивних інформаційних загроз на психіку та поведінку людини; психологічних механізмів переконання та навіювання; ролі інформаційних операцій і комунікаційних технологій у формуванні громадської думки; специфіки загроз інформаційній безпеці України у політичній, соціальній, економічній, гуманітарній та технологічній сферах; місця та значення інформаційної безпеки в системі національної безпеки;

– продемонструвати здатність ідентифікувати та аналізувати інформаційні, психологічні та технічні загрози; оцінювати рівень інформаційної вразливості особи, соціальних груп та інституцій; обирати відповідні методи протидії інформаційно-психологічному впливу; застосовувати засоби критичного мислення та інформаційного аналізу при роботі з даними, медіа-контентом та комунікаційними повідомленнями;

– продемонструвати практичні навички аналітичного і критичного мислення; виявлення маніпулятивних загроз у міжособистісній та публічній комунікації; оцінювання ідей і аргументації в інформаційних матеріалах; формулювання обґрунтованих висновків; розроблення заходів щодо підвищення інформаційної стійкості індивідів, організацій та соціальних спільнот; створення та впровадження пропозицій щодо підвищення рівня інформаційної безпеки та ефективності комунікації в професійній діяльності.

4. Структура курсу

ЛЕКЦІЇ

Тема 1. Сутність та зміст інформаційних загроз у сучасних умовах державотворення

1.1. Поняття інформаційних, інформаційно-психологічних та інформаційно-технічних загроз

1.2. Об'єкти, суб'єкти та цілі застосування інформаційних загроз у процесах державотворення

1.3. Інформаційні загрози в контексті державотворчих процесів: сфери ураження та механізми впливу

1.4. Види інформаційних загроз та їх наслідки для державотворення

Тема 2. Історія та сучасний стан інформаційних загроз

2.1. Витоки інформаційних загроз

2.2. Інформаційні загрози XX століття

2.3. Інформаційні загрози цифрової епохи

2.4. Сучасний стан і тенденції розвитку інформаційних загроз

Тема 3. Інформаційне протиборство та інформаційні операції

3.1. Сутність, принципи та форми інформаційного протиборства

3.2. Політичні, економічні, дипломатичні, технологічні та військові засоби інформаційного впливу

3.3. Інформаційно-психологічні операції та їх структурні елементи
3.4. Інформаційна інфраструктура як об’єкт впливу і захисту

Тема 4. Інформаційна війна, пропаганда та інформаційний тероризм
4.1. Інформаційна війна як форма гібридного протистояння
4.2. Завдання ІВ: дестабілізація, маніпулювання, розпалення конфліктів, зміна цінностей
4.3. Сім складових інформаційної війни
4.4. Інформаційний тероризм та комп’ютерна злочинність: загрози й механізми реалізації

Тема 5. Стратегії та інструменти протидії інформаційним загрозам
5.1. Загрози інформаційній безпеці України в різних сферах
5.2. Методи протидії інформаційно-психологічному впливу та дезінформації
5.3. Підвищення інформаційної стійкості: індивідуальний, груповий і державний рівні
5.4. Розроблення комплексних заходів із забезпечення інформаційної безпеки

ПРАКТИЧНІ ЗАНЯТТЯ

1. Сутність та зміст інформаційних загроз у сучасних умовах державотворення
2. Історія та сучасний стан інформаційних загроз
3. Інформаційне протиборство та інформаційні операції
4. Інформаційна війна, пропаганда та інформаційний тероризм
5. Стратегії та інструменти протидії інформаційним загрозам

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

Індивідуальне завдання полягає в підготовці письмової роботи, яка складається з чотирьох послідовно викладених частин, які нумеруються.

1 частина. **Визначення сутності інформаційного впливу**. Навести декілька визначень поняття «інформаційний вплив», «інформаційно-психологічний вплив», «інформаційно-технічний вплив», «інформаційні загрози» з вказанням джерела (автор, назва публікації – стаття в журналі, навчальний посібник, монографія тощо).

2 частина. **Глосарій дисципліни «Протидія інформаційним загрозам в сучасних умовах державотворення».** Навести перелік не менше як 10 понять (більш кількість дозволить отримати вищі бали), які розкривають зміст дисципліни. Потрібно навести поняття та визначити їх сутність.

3 частина «Фахівець майбутнього» в сфері інформаційних загроз. Стисло викласти інформацію вашого бачення стосовно того, яким має бути «Фахівець майбутнього» в сфері інформаційної загроз.

4 частина. **Ключові слова**. Навести перелік не менше як 10 ключових слів, які ви використовували у своїй роботі. Ключове слово – важливий елемент, який дозволяє деталізувати поняття. Ключові слова потрібно просто перерахувати, не надаючи їх визначення.

Під час презентації і захисту результатів виконання індивідуального завдання у межах практичних занять передбачено процедуру peer-assessment (оцінювання з боку інших здобувачів освіти).

5. Технічне обладнання та/або програмне забезпечення

На лекційних заняттях обов'язково мати з собою ґаджети зі стільниковим інтернетом.

Активований аккаунт університетської пошти (student.i.p@nmu.one) на Microsoft Office365.

Перевірений доступ з ПК чи мобільного ґаджету до за стосунків Microsoft Office: Teams, Moodle.

Інстальований на ПК та мобільних ґаджетах пакет програм Microsoft Office (Word, Excel, Power Point).

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

Загальні критерії досягнення результатів навчання відповідають описам 6-го кваліфікаційного рівня НРК.

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни **на підставі поточного оцінювання знань** за умови, якщо набрана кількість балів складатиме не менше 60 балів. Максимально за поточною успішністю здобувач вищої освіти може набрати 100 балів.

Теоретична частина оцінюється за результатами поточного тестування під час лекції на останньому тижні навчання. Поточний тест складається з 20 закритих тестових запитань, кожне з яких має одну правильну відповідь. За кожну правильну відповідь нараховується 2 бали. Загалом за поточне тестування отримується максимум **40 балів**.

Практична частина оцінюється за результатами:

- участі у практичних заняттях (відповіді на запитання, участь у дискусії, командна робота, рольові ігри, презентація окремого питання, що розглядається в межах заняття тощо); при несвоєчасному виконання практичних завдань оцінка знижується вдвічі; загалом за наскрізне завдання отримується максимум 40 балів;
- виконання, публічної презентації та захисту (відповіді на запитання, дискусія) результатів індивідуального завдання; за результатами публічної презентації отримується максимум 20 балів.

У сумі за практичну частину курсу при поточному оцінюванні отримується максимум **60 балів.**

Отримані бали за теоретичну та практичну частини додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за поточною успішністю здобувач вищої освіти може набрати **100 балів.**

Розподіл максимальної кількості балів за складовими поточного контролю:

Теоретична частина	Практична частина	**Разом**
40	60	**100**

6.3. Критерії підсумкового оцінювання: у випадку якщо здобувач вищої освіти за поточною успішністю отримав менше 60 балів та/або прагне поліпшити оцінку проводиться

підсумкове оцінювання (диференційований залік) під час сесії. Якщо здобувач не здав у письмовій формі виконане індивідуальне завдання, він отримує незадовільну підсумкову оцінку з дисципліни.

Залік проводиться у вигляді комплексної контрольної роботи, яка включає запитання з теоретичної та практичної частини курсу. Білет складається з **20 тестових завдань з теоретичної частини** із чотирма варіантами відповідей, одна правильна відповідь оцінюється в 2 бали (разом 40 балів) та 12 тестових завдань з практичної частини, кожне з завдань оцінюється максимум у 5 балів (разом 60 балів), причому:

− 5 балів – відповідність еталону;

− 4 бали – відповідність еталону з незначними помилками;

− 3 бали – часткова відповідність еталону, питання розкрито не повною мірою;

− 2 бали – наведено лише загальне розуміння питання, відповідь неповна та містить значні помилки;

− 1 бал – невідповідність еталону, але відповідність темі запитання;

− 0 балів – відповідь не наведена або не відноситься до теми запитання.

Отримані бали за відкриті та закриті тести додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за підсумковою роботою здобувач вищої освіти може набрати 100 балів.

7. Політика курсу

7.1. Політика щодо академічної доброчесності. 7.1. Політика щодо академічної доброчесності. Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів) що можуть використовуватися в освітньому процесі. Політика щодо академічної доброчесності регламентується положенням «Положення про систему запобігання та виявлення плагіату у Національному технічному університеті «Дніпровська політехніка»: https://old.nmu.org.ua/ua/content/activity/us_documents/Положення_запобіг_виявл_плагіат-2025.pdf .

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

Політика щодо використання штучного інтелекту під час опанування курсу регламентується відповідними нормами «Політики щодо використання штучного інтелекту в діяльності Національного технічного університету «Дніпровська політехніка»: https://old.nmu.org.ua/ua/content/activity/us_documents/Політика_ШІ_2025.pdf.

7.2. Комунікаційна політика.

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Обов’язком здобувача вищої освіти є перевірка один раз на тиждень (щонеділі) поштової скриньки на Office365 та відвідування групи дисципліни у Microsoft Teams.

Рекомендуємо створити профілі та підписатися на сторінку кафедри державного управління і місцевого самоврядування у Facebook: https://www.facebook.com/kafedra.publicmanagement/.

Протягом тижнів самостійної роботи обов’язком здобувача вищої освіти є робота у рамках дисципліни дистанційно у застосунку Microsoft Teams та на корпоративній платформі Moodle (www.do.nmu.org.ua).

Усі письмові запитання до викладача стосовно дисципліни мають надсилатися на університетську електронну пошту або до групи у Microsoft Teams.

7.3. Політика щодо перескладання.

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4. Відвідування занять.

Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим.

Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, відрядження, які необхідно підтверджувати документами у разі тривалої (два тижні) відсутності.

Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

Якщо здобувач вищої освіти захворів, ми рекомендуємо залишатися вдома і навчатися за допомогою дистанційної платформи.

Здобувачу вищої освіти, чий стан здоров'я є незадовільним і може вплинути на здоров'я інших здобувачів вищої освіти, буде пропонуватися залишити заняття (така відсутність вважатиметься пропуском з причини хвороби).

Оцінки неможливо отримати під час консультацій або інших додаткових годин спілкування з викладачем. За об'єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись дистанційно - в онлайн-формі, за погодженням з викладачем.

7.5. Політика щодо оскарження оцінювання. Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може оскаржити виставлену викладачем оцінку у встановленому порядку.

7.6. Зарахування результатів навчання, які отримані у неформальній освіті. Здобувачі вищої освіти має право на зарахування результатів навчання, які отримані у неформальній освіті, за окремими темами або видами навчальної активності із попереднім погодженням з викладачем дисципліни та гарантом освітньої програми. Визнання результатів здійснюється за наявності відповідних сертифікатів.

7.7. Участь в анкетуванні.

Наприкінці вивчення курсу та перед початком сесії здобувачам вищої освіти буде запропоновано анонімно заповнити електронні анкети (MS Forms). Посилання на форму буде розміщено у Teams курсу. Заповнення анкет є важливою складовою вашої навчальної активності, що дозволить оцінити дієвість застосованих методів викладання та врахувати ваші пропозиції стосовно покращення змісту навчальної дисципліни

8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основні

1. Биченок Н.Н., Савченко В.А., Дзюба Т.М. Основи забезпечення інформаційної безпеки держави у воєнній сфері : Підручник. 2017. URL: http://www.dut.edu.ua/ua/lib/1/category/742/view/2011

2. Бурячок В. Л., Толюпа С.В., Семко В.В., Складанний П.М., Лукова-Чуйко Н.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби посібник. К. : ДУТ-КНУ, 2016. 178 с. URL: http://www.dut.edu.ua/uploads/p_303_92597962.pdf

3. Бурячок, В.Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : Підручник; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с. URL: http://www.dut.edu.ua/uploads/l_1209_69915296.pdf

4. Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін. Інформаційна безпек особистості, суспільства, держави: Підручник. – К.: Видавничо-поліграфічний центр “Київський університет”, 2008.– 274 с.

5. Інформаційно-психологічне протиборство (еволюція та сучасність): Монографія / Я.М. Жарков, В.М. Петрик, М.М. Присяжнюк та ін. – К.: ПАТ «Віпол», 2013. – 248 с.

6. Остроухов В. В, Присяжнюк М. М, Фармагей О. І, Чеховська М. М. та ін.; під ред. Остроухова В. В. Інформаційна безпека. Підручник К.: Вид-во Ліра-К, 2021. 412 с. URL: https://duikt.edu.ua/uploads/l_1352_84114000.pdf

Нормативні документи

1. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 8 лютого 2021 р. № 92. URL: https://zakon.rada.gov.ua/laws/show/92-2021-%D0%BF#Text

2. Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 23 лютого 2006 р. № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

3. Про Доктрину інформаційної безпеки України : Указ Президента України від 25 лютого 2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text

4. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах : Постанова Кабінету Міністрів України від 16 листопада 2002 р. № 1772. URL: https://zakon.rada.gov.ua/laws/show/1772-2002-%D0%BF#Text

5. Про медіа : Закон України від 13 грудня 2022 р. № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text

6. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

7. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 9 січня 2007 р. Відомості Верховної Ради України. 2007. № 12. Ст. 102. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text

Додаткові

1. Мужанова Т.М., Якименко Ю.М. Досвід Європейського Союзу з протидії деструктивній інформаційній діяльності в мережі Інтернет. Сучасний захист інформації. 2019. № 2. С.37-41. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/2314

2. Теорія та практика сучасного інформаційно-психологічного протиборства: навчальний посібник. /В. В. Петрик, С. О. Гнатюк, М. М. Присяжнюк та ін. Полтава, 2022. 328 с.

3. Ананьїн В. О., Горлинський В. В., Пучков О. О. Міжнародна безпека та євроатлантична інтеграція України: навч. посіб. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2020. 231 с.

4. Інформаційна безпека: підручник /В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін; під. ред. В. В. Остроухова. Київ : Вид-во Лира-К, 2021. 412 с. URL: https://lira-k.com.ua/preview/12867.pdf

5. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 “Управління інформаційною безпекою“, 125 “Кібербезпека“/ В.І. Гур’єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин : ФОП Лук’яненко В.В. ТПК “Орхідея“, 2018. 166 с.

6. Менеджмент інформаційної безпеки: навчальний посібник для студентів спеціальності 125 "Кібербезпека" /О. Г. Корченко, М. Є. Шелест, С. В. Казмірчук,122 Ю. М. Ткач, Є. В. Іванченко. Ніжин: ФОП Лук'яненко В. ТПК "Орхідея", 2019. 408 с. URL: https://ir.stu.cn.ua/handle/123456789/19244

7. Менеджмент інформаційної безпеки: навчальний посібник для студентів спеціальності 125 "Кібербезпека" /О. Г. Корченко, М. Є. Шелест, С. В. Казмірчук, 122 Ю. М. Ткач, Є. В. Іванченко. Ніжин: ФОП Лук'яненко В. В. ТПК "Орхідея", 2019. 408 с. URL: https://ir.stu.cn.ua/handle/123456789/19244

Інформаційні ресурси

1. Верховна Рада України: офіційний веб-портал. URL: http://rada.gov.ua/

2.Президент України: офіційне Інтернет-представництво. URL: http://www.president.gov.ua/

3. Головний правовий портал України. URL: http://www.ligazakon.ua/

4. Кабінет Міністрів України: офіційний веб-портал. URL: http://www.kmu.gov.ua

5. Національне агентство України з питань державної служби: офіційний веб-портал. URL: http://www.nads.gov.ua.

6. Державна служба спеціального зв'язку та захисту інформації: [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua

5. Команда реагування на комп'ютерні надзвичайні події України: [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/

6. SAE Standards [Electronic Resource], Mode of access: World Wide Web., URL: http://standards.sae.org.

7. Інститут перспективного вивчення інформаційних війн (IASIW) URL: https://web.archive.org/web/20070709005214/http://www.psycom.net/iwar.1.html