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

Кафедра теорії та практики управління

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Робоча програма навчальної дисципліни (Силабус)

1. Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*28 Публічне управління та адміністрування*
Спеціальність	*281 Публічне управління та адміністрування*
Освітня програма	***Адміністративний менеджмент***
Статус дисципліни	*Нормативна*
Форма навчання	*Заочна*
Рік підготовки, семестр	*3 курс, осінній семестр*
Обсяг дисципліни	*120 год (4 кредити ЄКТС) 14 годин лекцій, 10 годин семінарських/практичних занять, 96 годин СРС*
Семестровий контроль/ контрольні заходи	Залік Модульна контрольна робота Домашня контрольна робота
Розклад занять	*https://schedule.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лектор: кандидат юридичних наук, старший викладач Дяковський Олександр Сергійович, o.dyakovskiy@gmail.com* *Семінарські, комп'ютерний практикум: Архипова Євгенія Олександрівна, к.філос.н., доцент, evgar55@gmail.com*
Розміщення курсу	Google classroom

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Навчальна дисципліна належить до нормативних дисциплін, які пропонуються до опанування здобувачам першого (бакалаврського) рівня вищої освіти за освітньою програмою «Адміністративний менеджмент».

Метою навчальної дисципліни є формування у здобувачів розуміння інформаційної безпеки як складного багаторівневого явища, що має соціальні, психологічні й технічні виміри.

Предметом навчальної дисципліни є теоретичні та практичні аспекти інформаційної безпеки. Зокрема студенти отримають розвинуть навички виявлення і протидії інформаційним загрозам на рівні людини, суспільства та держави, ознайомляться з нормативно-правовими актами, спрямованими на забезпечення інформаційних прав та свобод людини і громадянина та захист інтересів держави в інформаційній сфері, розвинуть навички забезпечення захисту приватності в повсякденному житті та професійній діяльності.

Навчальна дисципліна у комплексі з іншими освітніми компонентами сприяє розвитку таких програмних компетентностей та програмних результатів навчання[1] :

[1] мається на увазі, що цей освітній компонент забезпечує формування даних компетентностей та програмних

- програмні компетентності:

1. (ЗК 02)[2] Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
2. (ЗК 03) Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
3. (ЗК 04) Здатність бути критичним і самокритичним.
4. (ЗК 09) Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
5. (ФК 03) Здатність забезпечувати дотримання нормативно-правових та морально-етичних норм поведінки.
6. (ФК 13) Здатність до ідентифікації, оцінювання та управління реальними та потенційними ризиками та загрозами безпеки життєдіяльності людини, держави і суспільства

- програмні результати навчання:

7. (ПРН 11) Уміти здійснювати пошук та узагальнення інформації, робити висновки і формулювати рекомендації в межах своєї компетенції.
8. (ПРН 18) Забезпечувати формування безпечних умов функціонування людини, суспільства, держави

Навчальна дисципліна орієнтована на розвиток загальної інформаційної культури, критичного мислення та громадянської свідомості студентів, а також на формування професійних знань фахівців з публічного управління та адміністрування у сфері інформаційної безпеки.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

За структурно-логічною схемою підготовки фахівця дана навчальна дисципліна тісно пов'язана із обов'язковою дисципліною циклу професійної підготовки «Основи електронного урядування». Отримані теоретичні знання та практичні навички сприяють кращому розумінню дисциплін, що вивчатимуться пізніше, зокрема дисципліни «Державні інформаційні ресурси та електронні послуги».

3. Зміст навчальної дисципліни

Тема 1 Інформаційна безпека як складова національної безпеки

Тема 2. Інформація та інформаційне суспільство

Тема 3. Інформаційна безпека, безпека інформації та кібернетична безпека.

Тема 4. Захист приватності.

Тема 5. Маніпулювання інформацією.

Тема 6. Інсайдерство та соціальна інженерія.

результатів навчання разом із іншими освітніми компонентами, визначеними в ОПП у Матриці відповідності програмних компетентностей компонентам освітньої програми та Матриці забезпечення програмних результатів навчання відповідними компонентами освітньої програми.

[2] у дужках після номеру подано шифр компетентності чи результату навчання згідно з ОПП.

Тема 7. Інформаційне протиборство та інформаційні війни.

4. Навчальні матеріали та ресурси

Базові джерела:

Управління інформаційною безпекою. Конспект лекцій : навчальний посібник для студентів спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с. URL: https://ela.kpi.ua/handle/123456789/43377 (дата звернення 10.05.2025).

Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с. URL: https://er.nau.edu.ua/bitstream/NAU/57731/1/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_%D0%BA%D1%83%D1%80%D1%81%20%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D0%B9_2022.pdf (дата звернення 10.05.2025).

Інформаційна безпека : навч. посібн.; за заг. ред. Ю. Я. Бобало, І. В. Горбатого. Львів : вид-во Львовської політехніки, 2019. 580 с. URL: https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf (дата звернення 10.05.2025).

Основні нормативно-правові акти:

Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL: http://zakon4.rada.gov.ua/laws/show/2297-17 (дата звернення 10.05.2025)

Закон України «Про інформацію» від 02.10.1992 № 2657-XII. URL: http://zakon4.rada.gov.ua/laws/show/2657-12 (дата звернення 10.05.2025)

Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII. URL: http://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення 10.05.2025)

Закон України «Про основні засади забезпечення кібербезпеки України», від 05.10.2017. URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 10.05.2025)

Закон України «Про національну програму інформатизації» від 01.12.2022 № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#n191 (дата звернення 10.05.2025)

Стратегія інформаційної безпеки України; затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення 10.05.2025)

Стратегія кібербезпеки України: Безпечний кіберпростір – запорука успішного розвитку країни, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення 10.05.2025)

Додаткові джерела:

Архипова Є.О., Черниченко А.В. Забезпечення інформаційної безпеки в органах державної влади як нагальна потреба сьогодення. *Держава та регіони. Серія: Державне управління*. 2018. № 4 (64). С. 231-234. URL: http://www.pa.stateandregions.zp.ua/archive/4_2018/44.pdf (дата звернення 10.05.2025).

Архипова Є.О. Забезпечення інформаційної безпеки та захисту інформації: методичні аспекти. *Публічне управління та адміністрування: збірник наукових праць*. К.: НТУУ «КПІ», 2015. С.21-32.

Архипова Є.О. Теоретична сутність та практика використання асиметричної відповіді в умовах гібридної агресії. *Інвестиції: практика та досвід*. 2016. №24. С. 125-129. URL: http://www.investplan.com.ua/?op=1&z=5311&i=25 (дата звернення 10.05.2025).

Прудеус М. Основи маніпуляції : Відео-курс, 2022. URL: https://www.youtube.com/playlist?list=PL8G81iuosceius5hg2F9JQUx8oQaFfcdY (дата звернення 10.05.2025).

Інформація про інші основні та додаткові матеріали або посилання на матеріали чи ресурси, потрібні для вивчення навчальної дисципліни, публікується у гугл-класі.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

При викладанні дисципліни використовуються різні групи методів, зокрема словесні (розповідь, бесіда, пояснення, дискусія, коментування тощо), наочні (ілюстрування, презентації, слайди, схеми тощо), практичні (аналіз ситуацій, кейс-стаді, ділові ігри, робота з текстом, мозковий штурм. Також використовуються методи проблемних ситуацій, демонстрації пошукової діяльності, активізуючих запитань, навмисної помилки. В ході опанування дисципліни використовуються методи індивідуальної та групової роботи. В процесі навчання використовуються сервіс відеоконференцій Zoom, месенджери, Електронний кампус КПІ, також застосовуються різноманітні цифрові інструменти (зокрема, додатки Google Workspace, Miro, Canva, сервіси онлайн-тестування тощо).

Завдання та методичні рекомендації до виконання практичних робіт, питання до МКР, підсумкового контролю та інші матеріали викладаються в гугл-класі.

Орієнтовний перелік питань, що виносяться на лекційні, семінарські (практичні) заняття та СРС наведено нижче.

Лекційні заняття

Лекція 1. Інформаційна безпека як складова національної безпеки

1. Визначення та зміст поняття «інформаційна безпека».
2. Концепція національної безпеки України.
3. Роль та місце інформаційної безпеки в системі національної безпеки.
4. Захист життєво важливих інтересів держави в інформаційній сфері.

Завдання на СРС: надайте класифікацію національних інтересів.

Лекція 2. Інформаційна безпека та безпека інформації

1. Відмінність понять інформаційна безпека та безпека інформації.
2. Основні напрямки інформаційної безпеки.
3. Інформаційне протиборство та конфлікти, інформаційна війна, інформаційна зброя.
4. Принципи, головні задачі та функції забезпечення захисту інформації.
5. Національна система захисту інформації.

Завдання на СРС: охарактеризуйте стан та проблеми внутрішніх та зовнішніх відносин в інформаційній сфері.

Лекція 3. Кібернетична безпека

1. Поняття кібернетичної безпеки. Підходи до визначення кібернетичної безпеки.

2. Співвідношення термінів «кібербезпека» та «інформаційна безпека».
3. Стратегія кібербезпеки України.
4. Загрози кібербезпеці та загрози критичній інфраструктурі. Точки перетину. Кіберзлочин та кіберзлочинність.

Завдання на СРС: знайдіть в наукових джерелах визначення кібербезпеки та кіберзагроз та проаналізуйте ці визначення.

Лекція 4. Персональні дані. Право на приватність

1. Нормативно-правова база у сфері захисту персональних даних.
2. Персональні дані як об'єкт захисту. Персональних дані та конфіденційна інформація.
3. Суб'єкти відносин, пов'язаних із персональними даними. Їх права та обов'язки.
4. Зміст поняття «персональні дані». Види персональних даних.
5. Вимоги до обробки персональних даних.
6. Міжнародні акти із захисту персональних даних та захисту приватності.

Завдання на СРС: Визначте, які дані відносяться до чутливих персональних даних.

Лекція 5. Маніпулювання

1. Сутність, особливості та причини маніпулювання інформацією.
2. Підготовка та проведення маніпуляцій інформацією.
3. Основні засоби маніпуляції суспільною свідомістю.
4. Прийоми і технології маніпулювання при особистому спілкуванні.
5. Способи маніпулювання в мас-медіа.

Завдання на СРС: пошук підзаконних актів з регулювання інформаційних відносин в певній сфері діяльності.

Лекція 6. Інсайдерство та соціальна інженерія

1. Інсайдерство та інсайдери. Види інсайдерів.
2. Соціальна інженерія: зміст поняття.
3. Приклади реалізації соціоінженерних атак.

Завдання на СРС: Кевін Мітнік про соціальну інженерію.

Лекція 7. Інформаційне протиборство та інформаційна війна

1. Інформаційне протиборство та його види.
2. Інформаційна війна. Інформаційна зброя.
3. Поняття гібридної війни та гібридної агресії.
4. Спеціальні інформаційні операції.

Завдання на СРС: Наведіть історичні приклади гібридних війн.

Семінарські заняття

Семінарське заняття 1. Вступ до інформаційної безпеки

1) Актуальність інформаційної безпеки в сучасному суспільстві.
2) Інформаційна безпека як складова національної безпеки.
3) Складові інформаційної безпеки.
4) Проблеми розуміння інформаційної безпеки в професійних колах та на рівні суспільної свідомості. Інформаційна безпека та безпека інформації.
5) Соціальні аспекти інформаційної безпеки.
6) Загальне розуміння технічних аспектів інформаційної безпеки.

Завдання на СРС: Перелічіть загрози інформаційній безпеці особи.

Семінарське заняття 2. Державна інформаційна політика

1. Національний інформаційний суверенітет.
2. Сутність та завдання національної інформаційної політики.
3. Структура та завдання органів у сфері державної інформаційної політики України.
4. Національна програма інформатизації.
5. Інформаційна політика зарубіжних країн (доповіді по різним країнам).

Завдання на СРС:

Розкрити основні положення ЗУ «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки».

Продумати тези дискусії на тему «Інформаційний суверенітет : від захисту національної безпеки до обмеження інформаційних свобод».

Семінарське заняття 3. Інформація, інформаційні процеси і системи

1. Сутність та види інформації.
2. Атрибутивна та функціональна концепції інформації
3. Види інформації. Класифікація інформації за режимом доступу.
4. Соціальна інформація та її характеристики.
5. Міри інформації.
6. Проблеми визначення цінності інформації.
7. Інформаційні процеси і системи: основні поняття та визначення.

Завдання на СРС: Порівняйте поняття «цінність інформації» та «корисність інформації». В чому полягає глобальний характер інформатизації? Визначте поняття «сучасні інформаційні системи».

Семінарське заняття 4. Інформаційне протиборство. Спеціальні інформаційні операції

1. Інформаційне протиборство як форма забезпечення інформаційної безпеки
2. Визначення та концепція інформаційної війни
3. Органи та основні форми інформаційної війни
4. Визначення, особливості та сфера застосування інформаційної зброї

5. Сутність та завдання спеціальних інформаційних операцій (СІО).
6. Види та методи СІО.
7. Практичний досвід проведення СІО.

Завдання на СРС: основні форми інформаційної війни на державному рівні
Механізм реалізації психологічного впливу. Закономірності психологічного впливу
Порівняйте СІО, які проводяться на макро- і мікрорівні.

6. Самостійна робота студента

Студенти заочної форми навчання опановують самостійно весь матеріал, який не було розглянуто на лекціях та практичних / семінарських заняттях, але винесено на підсумковий та модульний контроль (див. додаток А).

Орієнтовне планування здобувачем освіти свого часу (академічних годин) на виконання окремих робіт СРС з навчальної дисципліни

№ з/п	Вид роботи студента /студентки	Норма часу, год.	Кількість	Всього, годин
1.	Підготовка до лекції	0,5	7	3,5
2.	Підготовка до практичного заняття	1	5	5
3.	Інші види СРС, робота з літературою та навчальними ресурсами за темами	8,2	7	57,5
4.	Підготовка до МКР	4	1	4
5.	Підготовка до ДКР	20	1	20
6.	Підготовка до заліку	6	1	6
	Всього			96

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Система оцінювання орієнтована на отримання балів за засвоєння теоретичних знать, розвиток практичних умінь та навичок, а також на стимулювання активності студентів. Вітається вільне висловлювання студентами своєї позиції щодо питань, які розглядаються на заняттях, та самостійний пошук додаткової інформації. Відносини між студентами та викладачем здійснюється на партнерських началах.

Студенти можуть ініціювати внесення окремих питань/тем до розгляду на заняттях.

Основні матеріали або посилання на матеріали чи ресурси, потрібні для вивчення навчальної дисципліни, розміщуються у Google class. Матеріали чи ресурси для додаткового/поглибленого вивчення окремих питань розміщуються на Google-диску та/або шукаються студентами самостійно, що забезпечує розвиток навичок пошуку інформації та її критичного аналізу.

Заняття проводяться у синхронному режимі. У разі погіршення безпекових умов чи масових перебоїв з електроживленням можливо переведення занять в **асинхронний режим**.

Способи ліквідації заборгованостей, які виникли через певні форс-мажорні обставини, обговорюються в індивідуальному порядку.

Засоби комунікації

Каналами зв’язку є:

- гугл-клас (матеріали, завдання, загальні оголошення);
- ZOOM-конференції (консультації);
- телеграм-чат (загальні оголошення, питання, зворотний зв'язок);
- повідомлення в телеграмі (особисті питання);
- телефон (066-360-6416) (термінові, нагальні питання, які незручно вирішувати в месенджері);
- пошта: evgar55@gmail.com (резервний канал зв'язку).

Процедура оскарження результатів контрольних заходів

Студенти (індивідуально чи групою) мають можливість порушити будь-яке питання, яке стосується процедури проведення чи оцінювання контрольних заходів, і розраховувати на неупереджений його розгляд.

Академічна доброчесність та норми етичної поведінки

Політика та принципи академічної доброчесності, норми етичної поведінки студентів та викладачів визначені у Кодексі честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code .

Робота, у якій виявлено порушення принципів академічної доброчесності, не приймається. За таку роботу бали анулюються, а також можуть бути нараховані штрафні бали.

При використанні інструментів ШІ студенти мають враховувати "Політику використання штучного інтелекту для академічної діяльності в КПІ ім. Ігоря Сікорського" (розміщення: https://osvita.kpi.ua/node/1225), зокрема те, що використання ШІ для створення враження, що здобувач знає більше, ніж є насправді, є академічним порушенням.

Політикою дисципліни дозволено використовувати інструменти генеративного ШІ при підготовці до занять та виконанні окремих завдань з дисципліни. В той же час, студенти мають пам'ятати про обмеження, притаманні будь-яким системам ШІ. Студенти повинні ***сприймати згенерований ШІ текст критично***, що, окрім іншого, потребує достатнього для виявлення можливих помилок ШІ рівня розуміння матеріалу студентами. Категорично заборонено видавати згенеровані ШІ матеріали як результат власної самостійної роботи без подальшого опрацювання, перевірки та верифікації.

Завдання, які передбачають використання у вашій відповіді тексту з якогось (будь-якого) джерела, завжди матимуть пряму вказівку на те, що такий текст можна / треба використовувати.

У всіх інших випадках, навіть якщо на цьому прямо не наголошено, передбачається власна відповідь студента. Не переписуйте з інтернету та не використовуйте відповіді своїх колег – бережіть свою репутацію та власні бали.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: виконання завдань до практичних / семінарських занять, тестування, МКР, ДКР.

Семестровий контроль: залік.

РСО для студентів заочної форми навчання

Рейтинг студента з навчальної дисципліни складається з балів, які він отримує за:

1) Доповіді на семінарах з презентацією або тести-відпрацювання 3 бали * 4 шт = 12 балів
2) ДКР (пошук та ідентифікація маніпуляцій) – 16 балів.
3) МКР (тест) – 28 балів.
4) Залікова робота – 44 бали.

Студенти заочної форми навчання можуть приєднатися до гугл-класу та виконувати завдання стаціонару (всі чи деякі). У такому разі студент може не виконувати аналогічні завдання під час залікової сесії (бали за відповідні завдання будуть перезараховані).
Запропонована РСО(2) має на меті стимулювати активність студентів заочної форми, заохочує їх до систематичного вивчення дисципліни, дозволяє мати кращу включеність в освітній процес (матеріали, регулярний зворотній зв'язок тощо), що сприятиме кращому засвоєнню теоретичних знань та формуванню практичних навичок. Також завчасне виконання завдань зменшує обсяг роботи на заліково-екзаменаційній сесії, що особливо з огляду на можливе відключення електроенергії, повітряні тривоги та інші форс-мажори.

Критерії оцінювання складових РСО та додаткова інформація

1. Доповідь з презентацією готується по одному питанню серед числа винесених на семінар.

Критерії оцінювання доповідей:

- повна відповідь на питання; якісна презентація; студент вільно орієнтується в матеріалі, знає термінологію, наводить приклади – 2,7-*3 бали*;
- відповідь потребує невеликих уточнень, студент знає матеріал, наводить шаблонні приклади – *2,3-2,6 бали;*
- відповідь потребує суттєвих доповнень; студент плутається в термінології та не може відповісти на уточнюючі запитання, не може навести приклади – *1,8-2,2 бали*;
- відповідь не відповідає вищезазначеним вимогам – *0 балів*.

Тест-відпрацювання готується в межах одного семінарського заняття (12 тестових питань, які можуть охоплювати всі або тільки вибрані питання семінар). Вимоги щодо **тестів-відпрацювань** викладені в гугл-класі у розділі «Загальна інформація». Максимальна оцінка за тест – 3 бали.

2. Домашня контрольна робота

Метою ДКР є вивчення прийомів (технік) маніпулювання, розвиток практичних навиків їх викриття та ідентифікації в різних життєвих ситуаціях.

Термін здачі ДКР студентами заочної форми навчання – не пізніше ніж за 5 днів до семінару з цієї дисципліни на заліковій сесії.

Ваговий бал ДКР – 16 балів.

Критерії оцінювання:

- приклади повною мірою ілюструють заявлені маніпулятивні прийоми та відповідають всім встановленим вимогам, ДКР виконана вчасно – 15-16 балів;
- деякі приклади потребують додаткових пояснень, уточнень або їх опис не повною мірою розкриває особливості вказаних маніпулятивних прийомів. Приклади вирізняються різноманітністю – 12-14 балів;

- приклади досить однотипні, або їх опис погано розкриває сутність деяких заявлених маніпулятивних прийомів, або прикладів замало, або ДКР зроблена із несуттєвою затримкою (до 3 днів включно) – -9-11 балів.
- приклади однотипні, або їх опис погано розкриває сутність заявлених маніпулятивних прийомів, або наведена недостатня кількість прикладів та/ або ДКР зроблена із суттєвою затримкою – 4-8 балів.
- ДКР не зараховано, 0 балів.

Вимоги до ДКР наведені у Додатку Б.

3. Модульна контрольна робота

Ваговий бал – 28. Проводиться наприкінці семестру у формі тестування. В тесті використовуються закриті питання, кожне з яких оцінюється в 1 бал. Якщо за МКР набрано менше 60% від максимального балу, вона вважається незарахованою та оцінюється в 0 балів.

Орієнтовні питання для підготовки до МКР наведено в додатку А.

4. Залікова робота

Залікова робота включає набір тематичних завдань по кожній темі дисципліни. Тематичні завдання пропонуються у вигляді кейсів, відкритих питань, тестів тощо.

Загальні критерії оцінювання завдань залікової роботи наступні:

- високий рівень виконання завдання (всіх його пунктів), повна аргументація; творчий підхід для відповіді на відкриті питання та кейс-стаді, від 90% правильних відповідей на закриті питання – 90% від максимального балу;
- завдання виконано на достатньо високому рівні, допускаються окремі відхилення чи неточності, які студент / команда може виправити в процесі обговорення, надані відповіді на уточнюючі питання; від 75% правильних відповідей на закриті питання – 75% від максимального балу;
- всі пункти завдання виконані на достатньому рівні, відповідь шаблонна; якість опрацювання теоретичного матеріалу та володіння термінологією прийнятна, окремі тези відповіді складно інтерпретувати; або якісно виконані лише окремі пункти завдання; від 60% правильних відповідей на закриті питання – 60% від максимального балу.
- робота не відповідає вищезазначеним вимогам – *0 балів*.

Як вже зазначалось, в гугл-класі студенти-заочники можуть ознайомитись із тематичними завданнями студентів денної форми навчання. Багато залікових завдань для студентів заочної форми аналогічні поточним тематичним завданням студентів денної форми. За бажанням, заочники можуть виконувати окремі тематичні завдання стаціонару, тим самим зменшуючи своє навантаження на заліковій сесії.

Заохочувальні бали

Заохочувальні бали нараховуються за:

- повідомлення на семінарському занятті за результатами опрацювання новітньої наукової літератури – 4 бали;
- участь в конференції (за тематикою дисципліни) – до 6 балів.

- публікація статті (за тематикою дисципліни) – до 10 балів (також можливе зарахування відповідних самостійних робіт чи доповіді, що обговорюється в індивідуальному порядку).

Максимальна сума балів за семестр – 100.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

Онлайн-курси

Дистанційне навчання через проходження сторонніх онлайн-курсів за тематикою дисципліни допускається за умови погодження із викладачем. При пред'явленні сертифікату про проходження курсу та його програми студенту можуть бути зараховані бали за виконання певних поточних завдань (відповіді на семінарах, практичні завдання). При цьому контрольні заходи з дисципліни виконуються на загальних підставах.

Деякі онлайн-курси за тематикою дисципліни:
Інформаційна безпека https://prometheus.org.ua/course/course-v1:Internews+INFOS101+UA_2021_T3 (4 год. відео)

Інформаційна гігієна. Як розпізнати брехню в соцмережах, в інтернеті та на телебаченні – https://courses.prometheus.org.ua/courses/course-v1:Prometheus+IH101+2021_T3/about (1,5 кр, 4 год. відео).

Дезінформація: види, інструменти та способи захисту – https://courses.prometheus.org.ua/courses/course-v1:Prometheus+DISINFO101+2021_T2/about (4 год).

Цифрова безпека та комунікація в онлайні – https://vumonline.ua/course/digital-security-and-communication-online/ (0,2 кр, 6 год)

Захист персональних даних – https://study.ed-era.com/uk/courses/course/371/NaN (15 год.)

Захист персональних даних. Спеціалізований курс для державних службовців – https://study.ed-era.com/uk/dashboard/course?userCourseId=328870#!372 (6 год).

Фактчек: довіряй-перевіряй – https://courses.ed-era.com/courses/course-v1:VOXU-EdEra+FactCheck101+2018/about (15 год.)

Інклюзивне навчання

Навчальна дисципліна може викладатися для всіх студентів з особливими освітніми потребами. У разі потреби завдання можуть бути скориговані.

Орієнтовний перелік питань для підготовки до модульного та підсумкового контролю з дисципліни “Основи інформаційної безпеки”

1. Розкрийте сутність інформаційної безпеки як складової національної безпеки.
2. Поясніть, у чому полягає актуальність інформаційної безпеки в сучасному суспільстві.
3. Визначте основні напрями інформаційної політики України. Надайте коротку характеристику її нормативно-правового забезпечення.
4. Розкрийте поняття національного інформаційного суверенітету. Назвіть інструменти, які можуть використовуватися для його забезпечення.
5. Охарактеризуйте підходи до визначення поняття інформації. Назвіть види інформації.
6. Поясніть зміст атрибутивної та функціональної концепції інформації.
7. Розкрийте етапи життєвого циклу інформації.
8. Поясніть підходи до визначення цінності інформації.
9. Наведіть класифікацію інформації за видами, за порядком доступу, за ступенем секретності.
10. Охарактеризуйте сутність та значення інформаційних революцій для розвитку людства.
11. Визначте, у чому полягає глобальний характер інформатизації.
12. Надайте загальну характеристику концепцій інформаційного суспільства.
13. Охарактеризуйте основні риси та проблеми сучасного інформаційного суспільства.
14. Назвіть основні риси та тенденції розвитку суспільства знань. Порівняйте його із інформаційним суспільством.
15. Визначте сутність та наведіть класифікацію інформаційних загроз. Виокремте загрози, які характерні саме для сучасного інформаційного суспільства.
16. Надайте коротку характеристику загрозам інформаційної безпеки людини, суспільства та держави.
17. Порівняйте поняття “Інформаційна безпека”, “безпека інформації”, “кібернетична безпека”.
18. Назвіть складові інформаційної безпеки. Розкрийте соціальні аспекти інформаційної безпеки.
19. Розкрийте основні властивості інформації як об'єкту захисту.
20. Визначте сутність кібернетичної безпеки. Назвіть пріоритетні напрями забезпечення кібербезпеки в Україні.
21. Визначте зміст та критерії розмежування кіберпростору та інформаційного простору.
22. Поясніть зміст понять “кіберзлочин” та “кіберзлочинність”.
23. Розкрийте сутність персональних даних та захисту приватності. Поясніть співвідношення понять “персональні дані” та “конфіденційна інформація”.
24. Розкрийте права та обов'язки суб'єктів відносин, пов'язаних із персональними даними. Поясніть вимоги до обробки персональних даних.
25. Розкрийте зміст понять «приватність». Визначте спектр проблем захисту приватності.
26. Дайте визначення поняття “маніпулювання”. Назвіть ознаки маніпулювання.
27. Охарактеризуйте процес підготовки та реалізації маніпуляцій.
28. Розкрийте сутність та наведіть приклади використання технологій маніпулювання суспільною свідомістю.
29. Розкрийте сутність та наведіть приклади використання технологій маніпулювання індивідуальною свідомістю.
30. Поясніть зміст понять “соціальна інженерія” (як метод отримання інформації) та “соціальні хакери”, розкрийте алгоритм реалізації соціотехнічної атаки.
31. Охарактеризуйте методи соціальної інженерії. Розкрийте класифікацію та наведіть приклади соціоінженерних атак.
32. Поясніть сутність та механізми захисту від фішингу, вішингу, смішингу, фармінгу.
33. Розкрийте зміст поняття “інсайдерство”. Охарактеризуйте види інсайдерів.
34. Розкрийте зміст понять інформаційне протиборство, інформаційна війна, інформаційна зброя.

35. Надайте визначення, охарактеризуйте види та особливості інформаційної зброї.
36. Поясніть сутність і задачі спеціальних інформаційні операції. Аргументуйте відповідь прикладами.
37. Розкрийте технологію проведення спеціальних інформаційних операцій.
38. Поясніть сутність та особливості гібридної війни.

Додаток Б

Домашня контрольна робота з дисципліни
“Основи інформаційної безпеки”

Опис роботи
Метою ДКР є вивчення прийомів (технік) маніпулювання, розвиток практичних навиків їх викриття та ідентифікації в різних життєвих ситуаціях.

Студенти повинні підібрати по 6 прикладів застосування різних маніпулятивних прийомів чи технік. Приклади повинні бути різнопланові (на основі відеоматеріалів, графічних, текстових матеріалів тощо; рекламні, новинні, освітні, розважальні матеріали, ток-шоу тощо).
Всі приклади мають бути реальні та свіжі. Наприклад, якщо ви аналізуєте рекламний текст, ця реклама має демонструватися зараз; новинний, інформаційний матеріал – не старше 10 днів. Виключення – міжособистісні маніпуляції: наводячи приклад міжособистісних маніпуляцій, можна використовувати змодельовані ситуації (не більше 1 з 6 необхідних прикладів).

Повторення одного прикладу (конкретного) стосовно одного маніпулятивного прийому (техніки) не дозволяється.
Робота виконується в спільному гугл-документі.

Структура відповіді
Кожний приклад маніпулятивного прийому складається з:

- наскрізної нумерації прикладу, прізвища студента, дати та часу внесення прикладу в документ;
- опису матеріалу, який містить маніпуляцію. Це може бути фрагмент (текст) промови чи стенограма виступу (можна доповнювати відео чи аудіозаписом), **текстовий** опис відеоряду (також можна додати посилання на відео), фрагмент тексту (для друкованих матеріалів), опис ситуації тощо. Опис матеріалу повинен пояснювати, яким чином в цьому випадку реалізований маніпулятивний прийом/техніка. Текстовий опис може бути доповнений ілюстративним матеріалом (фотографія, стоп-кадр, рекламний постер тощо), посиланням на відео (із вказаням таймінгу, якщо загальний обсяг відео великий). Джерело має бути чітко ідентифіковано (наприклад, виступ ПІБ в політичному ток-шоу “ХХХ” від 7.11.23; реклама кави “Nescafe” на Інтері).
- за необхідності можна надати додаткові коментарі.

Якщо ви першим ілюструєте якусь маніпулятивну техніку (прийом), потрібно навести її назву та коротко викласти її суть (оформлення за шаблоном нижче).
Можна створювати і нові групи прийомів (нумерація першого рівня), але такі групи не повинні допускати дублювання прийомів. Наприклад, якщо якась із маніпулятивних технік універсальна (використовується і в рекламі, і в новинах, і в ток-шоу, то слід обрати загальну

рубрику – маніпуляції в ЗМІ; якщо ж даний прийом використовується тільки в рекламі, то обирайте/створюйте відповідну групу.

Зверніть увагу, що у одних і тих саме технік можуть бути різні назви, тому переглядайте, що створили до вас, і уникайте дублювань. Небажано наводити приклади на ті прийоми, на які є вже більше 8 прикладів.

Посилання на документ для спільної роботи буде надано перед початком виконання ДКР.

Робочу програму навчальної дисципліни (силабус):

Складено: доцентом кафедри теорії та практики управління, кандидатом філософських наук, доцентом

Архиповою Євгенією Олександрівною

Ухвалено кафедрою теорії та практики управління (протокол № 15 від 19.06.2025 р.)

Погоджено Методичною комісією факультету соціології і права (протокол № 4 від 24.06.2025 р.)