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	*С - соціальні науки, журналістика, інформація та міжнародні відносини*
Спеціальність	*С5 Соціологія*
Освітня програма	***Врегулювання конфліктів і медіація***
Статус дисципліни	*Вибіркова*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*3 курс, 5 семестр*
Обсяг дисципліни	*120 год (4 кредити ЄКТС)* *аудиторні заняття: лекції – 16 годин, практичні (семінарські) – 30 годин,* *самостійна робота – 74 години*
Семестровий контроль/ контрольні заходи	*Залік, МКР.*
Розклад занять	*rozklad.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 вивчення та результати навчання

Навчальна дисципліна належить до вибіркових дисциплін, які пропонуються до опанування здобувачам першого (бакалаврського) рівня вищої освіти.

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 здобувачі отримають та 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:

- програмні компетентності:

- 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.

- 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.

- Здатність бути критичним і самокритичним.

- Здатність вчитися і оволодівати сучасними знаннями.

- Здатність діяти соціально відповідально та свідомо.

- програмні результати навчання:

- Вміти використовувати інформаційно-комунікаційні технології у процесі пошуку, збору та аналізу соціологічної інформації.

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

Дисципліна «Основи інформаційної безпеки» є вибірковою дисципліною, яка може вивчатися студентами без будь-яких попередніх умов.

Дисципліна має міждисциплінарний характер та інтегрує відповідно до свого предмету спеціальні знання з інших освітніх і наукових галузей. Їй передують такі дисципліни як Загальна психологія, Інформаційні технології в проєктній діяльності, Соціологія тощо.

Для забезпечення освітнього процесу під час дистанційного навчання та більш ефективної комунікації з метою розуміння структури навчальної дисципліни і засвоєння матеріалу використовуються система Електронний кампус, ресурси платформи дистанційного навчання сервіси для організації онлайн-конференцій та відеозв'язку (наприклад, «Zoom»), електронна пошта, месенджери (WhatsApp, google документи). Також необхідно володіти навичками з використання текстового редактора, редактора зі створення презентацій, редактора зі створення таблиць.

3. Зміст навчальної дисципліни

Тема 1. Інформаційна безпека як складова національної безпеки.

Тема 2. Інформація, інформаційні процеси і системи. Інформаційне суспільство.

Тема 3. Інформаційна безпека та безпека інформації.

Тема 4. Кібернетична безпека.

Тема 5. Персональні дані.

Тема 6. Право на приватність та його захист.

Тема 7. Маніпулювання інформацією.

Тема 8. Інсайдерство та соціальна інженерія.

Тема 9. Інформаційне протиборство та інформаційна війна.

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 10.05.2024).

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 10.05.2024).

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 10.05.2024).

Основні нормативно-правові акти:

Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: http://zakon4.rada.gov.ua/laws/show/2297-17 (дата звернення 10.05.2024)

Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: http://zakon4.rada.gov.ua/laws/show/2657-12 (дата звернення 10.05.2024)

Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: http://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення 10.05.2024)

Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 10.05.2024)

Про національну програму інформатизації : Закон України від 01.12.2022 р. № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#n191 (дата звернення 10.05.2024)

Стратегія інформаційної безпеки України : затв. Указом Президента України від 28 груд. 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення 10.05.2024)

Стратегія кібербезпеки України: Безпечний кіберпростір – запорука успішного розвитку країни : затв.а Указом Президента України від 26 серп. 2021 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення 10.05.2024)

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 10.05.2024).

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 10.05.2024).

Прудеус М. Основи маніпуляції : Відео-курс, 2022. URL: https://www.youtube.com/playlist?list=PL8G81iuosceius5hg2F9JQUx8oQaFfcdY (дата звернення 10.05.2024).

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. Інформація, інформаційні процеси і системи. Інформаційне суспільство

1. Інформація, інформаційні процеси і системи: основні поняття та визначення.
2. Види інформації
3. Життєвий цикл інформації.
4. Соціальна суть інформації.
5. Глобальний характер інформатизації.
6. Становлення та розвиток концепцій інформаційного суспільства.
7. Загрози та виклики інформаційного суспільства.

Дидактичні засоби: схема «Види інформації».

Завдання на СРС: визначте сутність поняття «амбівалентність інформації».

Лекція 3. 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 4. 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 5. Персональні дані

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. Вимоги до обробки персональних даних.

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

Лекція 6. Право на приватність та його захист

1. Розвиток уявлень про право на приватність (приватне життя) та захист приватності.
2. Зміст поняття «персональні дані». Види персональних даних.
3. Міжнародні акти із захисту персональних даних та захисту приватності.
4. Вітчизняні нормативно-правові акти із захисту персональних даних та приватного життя.
5. Захист приватності в Інтернеті.

Завдання на СРС: Визначте внесок статті С. Уоррена та Л. Брандейса «Право на приватність» у розумінні питання захисту приватності.

Лекція 7. Маніпулювання інформацією

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 8. Інсайдерство та соціальна інженерія. Інформаційне протиборство та інформаційна війна

1. Інсайдерство та інсайдери. Види інсайдерів.
2. Соціальна інженерія: зміст поняття.
3. Приклади реалізації соціоінженерних атак.
4. Інформаційне протиборство та його види.
5. Інформаційна війна. Інформаційна зброя.
6. Поняття гібридної війни та гібридної агресії.
7. Спеціальні інформаційні операції.

Завдання на СРС: Кевін Мітник про соціальну інженерію. 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 суспільство та суспільство знань

1. Сутність та значення інформаційних революцій для розвитку людства.
2. Становлення та розвиток концепцій інформаційного суспільства (Д.Белл, М. Кастельс, Е. Тоффлер, Й. Масуда та ін) – доповіді за окремими авторами.
3. Суспільство знань: основні риси та тенденції.
4. Загрози та виклики інформаційного суспільства.
5. Дискусія: чи дійсно відбувається становлення нової людини (зміна мотивації, змісту праці тощо)?

Завдання на СРС: ознаки людини нового типу у працях науковців.

Семінарське заняття 5. Пошук та перевірка інформації

1. Пошук інформації в пошукових системах. Розширені інформаційні запити, фільтри, пошукові оператори.
2. Пошук інформації в академічних базах даних.
3. Пошук інформації в бібліотеках.
4. Критерії якості і достовірність джерела інформації. Оцінка за принципом CRAAP (актуальність, достовірність, авторитетність, точність, мета).
5. Методи перевірки автора інформації. Пошук даних про автора, аналіз його репутації та попередніх публікацій.
6. Виявлення фейків та дезінформації. Платформи для перевірки фактів (FactCheck, Snopes), інструментів для зворотного пошуку зображень (TinEye, Google Images).
7. Аналіз статистичної інформації та даних (виявлення маніпуляцій з цифрами, інтерпретації графіків, таблиць).
8. Фактчекінг.

Завдання на СРС: Завдання з інформаційного пошуку на тему кібернетичної безпеки (детальна інформація буде в гугл-класі).
Перелічіть ресурси, які викривають дезінформаційні кампанії рф

Семінарське заняття 6. Кібернетична безпека, кіберзагрози та кіберзахист

1. Поняття кібернетичної безпеки. Підходи до визначення кібернетичної безпеки. Співвідношення термінів «кібербезпека» та «інформаційна безпека».
2. Кіберпростір та інформаційний простір: критерії розмежування.
3. Об’єкти та суб’єкти забезпечення кібербезпеки.
4. Загрози кібербезпеці та загрози критичній інфраструктурі. Точки перетину. Кіберзлочин та кіберзлочинність.
5. Пріоритети та напрями забезпечення кібербезпеки України.
6. Національні стратегії кібербезпеки інших країн (декілька доповідей по стратегіям різних країн).

Завдання на СРС

Кореляція загроз кібернетичній безпеці із інформаційними загрозами людині, суспільству та державі.

Семінарське заняття 7. Загрози в інформаційній сфері

1. Основні визначення поняття «загроза». Визначення і джерела інформаційних загроз.
2. Класифікація інформаційних загроз.
3. Загрози інформаційній безпеці людини.
4. Загрози інформаційній безпеці суспільства.
5. Загрози інформаційній безпеці держави.
6. Загрози безпеці інформації. Основні загрози доступності, цілісності та конфіденційності.
7. Гучні приклади порушення інформаційної безпеки.

Завдання на СРС: приклади загроз доступності та цілісності інформації.

Семінарське заняття 8. Захист персональних даних та захист приватності

1. Зміст та обсяг поняття «персональні дані».
2. «Чутливі» персональні дані та їх обробка.
3. Доступ до персональних даних.
4. Розвиток уявлень про право на приватність (приватне життя) та захист приватності.
5. Складнощі визначення поняття приватного життя.
6. Основні категорії та терміни в сфері захисту персональних даних.
7. Організація захисту персональних даних.
8. Міжнародні акти із захисту персональних даних та захисту приватності.
9. Вітчизняні нормативно-правові акти із захисту персональних даних та приватного життя.

Завдання на СРС: проблеми захисту права на приватність користувачів інтернету.

Семінарське заняття 9. Захист приватності в мережі

1. Ризики приватності в інтернеті.
2. Захист права на приватність користувачів інтернету.
3. Налаштування приватності в поширених браузерах.
4. Особливості спілкування в соціальних мережах та правила листування електронною поштою.
5. Дискусія: чи можливо забезпечити приватність в інтернеті?

Завдання на СРС: проблеми захисту права на приватність користувачів інтернету.

Семінарське заняття 10. Маніпуляції свідомістю

1. Поняття та ознаки маніпулювання.
2. Підготовка та реалізація маніпуляцій.
3. Прийоми (техніки, технології) маніпулювання індивідуальною свідомістю
4. Прийоми (техніки, технології) маніпулювання масовою свідомістю
5. Маніпуляції в рекламі.
6. Маніпуляції в інших сферах.

Семінарське заняття 11-12. Інсайдерство та соціальна інженерія

1. Соціальна інженерія та соціальні хакери: зміст понять.

2. Методи соціальної інженерії.
3. Алгоритм соціотехнічної атаки.
4. Типи соціоінженерних атак та приклади реалізованих атак (аналіз сміття; особистісні підходи; реверсивна соціальна інженерія; фішинг, вішинг, смішинг, фармінг тощо. Можна декілька доповідей).
5. Приклади соціального програмування.
6. Інсайдерство та інсайдери. Види інсайдерів.
7. Загальні рекомендації щодо захисту від інсайдерських витоків інформації.
8. Джерела інсайдерської інформації (приклади).

Завдання на СРС: проблеми захисту права на приватність користувачів інтернету.

Семінарське заняття 13-14. Інформаційне протиборство. Інформаційна зброя

1. Основні поняття інформаційного протиборства: інформаційні протиборство, війна, тероризм, злочинність.
2. Інформаційне протиборство як форма забезпечення інформаційної безпеки
3. Визначення та концепція інформаційної війни
4. Органи та основні форми інформаційної війни
5. Визначення, особливості та сфера застосування інформаційної зброї
6. Інформаційна зброя воєнного та невоєнного застосування
7. Особливості, що характеризують основні риси застосування інформаційної зброї.
8. Заходи, способи та форми ведення інформаційної боротьби
9. Зміст психологічних операцій та ефективність психологічного впливу в них
10. Форми психологічної війни.
11. Сутність та завдання спеціальних інформаційних операцій.
12. Види СІО (спрямовані проти суб'єктів, які ухвалюють рішення; спрямовані на компрометацію, завдання шкоди опонентам; спрямовані на політичну (економічну) дестабілізацію).
13. Методи СІО: дезінформування; пропаганда; диверсифікація суспільної свідомості; психологічний тиск; розповсюдження чуток.
14. Практичний досвід проведення СІО (доповіді за різними 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.

Семінарське заняття 15. Модульна контрольна робота

Самостійна робота студента

Самостійна робота здобувача ВО в рамках освітнього компоненту включає комплекс тематичних питань для роздумів і практичних завдань, спрямованих на самоконтроль знань та організацію самопідготовки студентів в рамках кожного з практичних/семінарських занять і передбачає: підготовку до аудиторних занять, підготовку до модульної контрольної роботи, підготовку до заліку.

№ з/п	Самостійна робота студентів	Кількість годин
1	Підготовка до аудиторних занять	64

2	Підготовка до складання модульної контрольної роботи	4
3	Підготовка до заліку	6
	Всього	74

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 здобувачів. Вітається вільне висловлювання здобувачами своєї позиції щодо питань, які розглядаються на заняттях, та самостійний пошук додаткової інформації. Здобувачі 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 знаходяться здобувачами самостійно, що забезпечує розвиток навичок пошуку інформації та її критичного аналізу.

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

Протерміновані самостійні роботи у формі відкритих питань не відпрацьовуються. Можливо отримання балів за виконання протермінованих контрольних заходів, якщо вони проводились у формі закритих тестів (у такому разі доступ до тесту надається в індивідуальному порядку).

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

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

Календарний контроль

Проміжна атестація здобувачів денної форми навчання є календарним контролем. Метою проведення атестації є підвищення якості навчання здобувачів та моніторинг виконання графіка освітнього процесу здобувачами.

Академічна доброчесність та норми етичної поведінки

Політика та принципи академічної доброчесності, норми етичної поведінки здобувачів 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.

При використанні інструментів ШІ здобувачі 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. У той же час, здобувачі мають пам'ятати про обмеження, притаманні будь-яким системам ШІ. Здобувачі повинні сприймати згенерований ШІ текст критично, що, окрім іншого, потребує достатнього для виявлення можливих помилок ШІ рівня розуміння матеріалу здобувачами. 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 здобувача. 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: робота на практичних / семінарських заняттях, МКР.
Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.

Семестровий контроль: залік.

Рейтингова система оцінювання

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

№ з/п	Вид роботи	Ваговий бал	Кількість	Всього
1.	Виконання поточних завдань	6	10	60
2.	Доповіді на семінарах / тести-відпрацювання	3	4	12
3.	МКР (тест)	28	1	28
	Всього			**100**

Критерії оцінювання складових РСО та додаткова інформація

1. Робота на семінарських/практичних заняттях:

1. *Виконання поточних завдань*
   Поточні завдання, в т.ч. експрес-контрольні, проводяться за темою поточного чи

попереднього семінарів. Завдання та критерії оцінювання оголошуються безпосередньо перед контрольним заходом. Максимальна оцінка складає 6 балів. Кількість експрес-контролів – 10.

Загальні критерії оцінювання поточних завдань наступні.

- 6 балів - повна відповідність чек-листу оцінювання, виконані всі задачі завдання, студенти можуть пояснити та обґрунтувати відповідь, відповісти на уточнюючі питання – 90% від максимального балу.
- 5 балів - завдання виконано на високому рівні, виконані майже всі пункти згідно із чек-листом, допускаються окремі відхилення чи неточності, які студент може виправити в процесі обговорення – 75% від максимального балу.
- 4 бали - завдання виконано на мінімально достатньому рівні згідно із чек-листом, якість опрацювання матеріалів прийнятна – 60% від максимального балу.
- 0 балів - невиконанні завдання.

2. ***Доповіді на семінарах або тести-відпрацювання***

3 бали * 4 доповіді/теста = 12 балів.

Для рівномірного набрання балів протягом семестру студентам денної форми навчання рекомендується підготувати 2 доповіді/ 2 теста до першої атестації і 2 доповіді/теста у другій половині семестру.

Доповідь з презентацією готується по одному питанню серед числа винесених на семінар.
Критерії оцінювання доповідей:

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 – 12 балів.

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 не зарахованою та оцінюється в 0 балів.

Орієнтовні питання для підготовки до МКР наведено в додатку А.

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.

Атестація здобувачів денної форми навчання проводиться двічі за навчальний семестр (на 8 та 14 тижнях). Здобувач є атестованим, якщо його поточний рейтинг складає не менше половини максимально можливого балу на момент виставлення атестації. Орієнтовні максимальні бали на момент першої та другої атестації - 30 та 70 відповідно.

Максимальна сума балів за семестр – 100.

Для отримання заліку з навчальної дисципліни потрібно мати рейтинг не менш ніж 60 балів. Здобувачі, які наприкінці семестру мають рейтинг менше 60 балів, а також ті, хто хоче підвищити оцінку у системі ECTS, пишуть заліковий тест. При цьому попередній рейтинг студента з навчальної

дисципліни скасовується і він отримує оцінку з урахуванням результатів залікового тесту.

Заліковий тест містить 50 закритих питань, які формулюються на основі матеріалу, розглянутого на лекціях та семінарах. Орієнтовні питання для підготовки до залікової контрольної роботи наведено в додатку А. Одне питання тесту оцінюється у 2 бали, виконана залікова контрольна робота - 60% вірно виконаних тестових завдань. Максимальна оцінка за заліковий тест складає 100 балів.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Рейтингова оцінка здобувача (бали)	Університетська шкала оцінок рівня здобутих компетентностей (результатів навчання)
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно

Можливі відмітки у відомості семестрового контролю:

Не допущено	Невиконання умов допуску до семестрового контролю
Усунено	Порушення принципів академічної доброчесності або морально-етичних норм поведінки
Не з’явився	Здобувач, був допущений, але не з’явився на залік

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 здобувачу можуть бути зараховані бали за виконання певних поточних завдань. 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 здобувачів з особливими освітніми потребами. У разі потреби завдання можуть бути скориговані.

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 ФСП (протокол № 15 від 15.06.2025 р.)

Погоджено Методичною комісією факультету (протокол № 9 від 24.06.2025 р.)

Додаток А

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. Дайте 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. Дайте 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 з інформаційним суспільством.
15. Визначте сутність та наведіть класифікацію інформаційних загроз. Виокремте загрози, які характерні саме для сучасного інформаційного суспільства.
16. Дайте 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. Дайте 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.