**Силабус освітнього компонента**
Програма навчальної дисципліни

# Інформаційна безпека держави

**Шифр та назва спеціальності**
F5 – Кібербезпека та захист інформації

**Інститут**
ННІ комп`ютерних наук та інформаційних технологій

**Спеціалізація**

**Кафедра**
Кібербезпеки (328)

**Освітня програма**
Кібербезпека

**Тип дисципліни**
Обов'язкова

**Рівень освіти**
Перший (бакалаврський)

**Форма навчання**
Денна, заочна

**Семестр**
2

**Мова викладання**
Українська, англійська

## Викладачі, розробники

**КОРОЛЬ Ольга Григорівна**
olha.korol@khpi.edu.ua
кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 175, з яких 19 навчальних посібників, 74 статті у закордонних виданнях та фахових виданнях України, 18 патентів на корисну модель, 9 у наукометричній базі Scopus, гарант освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Національна безпека держави» , «Інформаційна безпека держави», «Комплексний тренінг «Безпека веб-застосунків»», у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

## Загальна інформація

### Анотація

Навчальна дисципліна "Інформаційна безпека держави" є обов'язковою навчальною дисципліною. Дисципліна спрямована на дослідження способів, методів, засобів і каналів реалізації загроз національним інтересам на інформаційному рівні та їх своєчасного виявлення, запобігання і нейтралізації.

## Мета та цілі дисципліни

Формування теоретичних основ законодавчої бази України та міжнародного суспільства в галузі національної та інформаційної безпеки держави, визначення основних вимог щодо формування підтримки та удосконалення систем управління інформаційної безпеки критичних інформаційно-комунікаційних систем, а також визначення місця і ролі інформаційної безпеки в загальній системі національної безпеки, стану та принципів забезпечення інформаційної безпеки особистості, суспільства та держави.

## Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

## Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК4. Здатність спілкуватися іноземною мовою.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
ЗК6. 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.
ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

## Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

### Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

### Передумови вивчення дисципліни (пререквізити)

Вступ до спеціальності. Ознайомча практика.

### Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

## Програма навчальної дисципліни

### Навчальні заняття

#### Лекції

| Теми лекцій | Кількість годин |
|---|---|
| **Тема 1. Поняття інформаційної безпеки держави та складових національних інтересів України в інформаційній сфері. Основні положення інформаційної безпеки.**<br>Цілі та завдання навчальної дисципліни «Інформаційна безпека держави». Місце дисципліни у навчальному процесі підготовки спеціаліста з кібербезпеки. Структура, зміст тематичного плану вивчення дисципліни; навчально-методична література. Особливості вивчення дисципліни; форми контролю знань, умінь та навичок здобувачів. Основні складові інформаційної безпеки держави. Класифікація видів інформаційної безпеки держави. Види інформаційної безпеки. Загрози інформаційній безпеці України. Доктрина інформаційної безпеки України. Пріоритети державної політики в інформаційній сфері. | 2 |
| **Тема 2. Загрози безпеці інформації.**<br>Дестабілізуючі фактори інформаційної безпеки. Класифікація загроз інформаційній безпеці. Актуальні загрози національній безпеці України. Маніпулювання свідомістю, сутність та види маніпуляції. Роль та місце маніпулювання в національних системах державного управління та політичних системах, а також у формуванні та здійсненні міжнародних стосунків. Сутність та прояви інформаційного насильства. Проблемні питання правового запобігання здійсненню інформаційного насильства. | 2 |
| **Тема 3. Основи інформаційного протиборства. Кібернетична зброя.**<br>Основні поняття інформаційного протиборства. Концепція інформаційної війни. Основи, форми та принципи кібернетичної розвідки. Основи кібернетичного впливу. Класифікація кібернетичної зброї. Основні завдання, що покладаються на кібернетичну зброю. Об'єкт кібернетичного впливу та його складові елементи. Методи та засоби застосування кібернетичної зброї. | 2 |
| **Тема 4. Психологічна війна та інформаційно-психологічна безпека держави.**<br>Основні поняття, цілі та завдання психологічної війни. Види психологічного впливу. Форми психологічної війни. Особливі способи та прийоми психологічної війни. Основи інформаційно-психологічної безпеки держави. | 2 |

| | |
|---|---|
| Принципи безпеки у психосфері. Сили та засоби інформаційно-психологічної безпеки. | |
| **Тема 5. Менеджент інформаційної безпеки.** Короткий огляд проблеми управління ризиками. Інтеграція управління ризиком у життєвий цикл розвитку систем (system development life cycle, sdlc). Життєвий цикл іт-систем. Методологія оцінки ризику. Зменшення ризиків. Загальна наслідність дій у методології зменшення ризиків. Аналіз рентабельності і залишковий ризик. Ключові фактори успішного управління ризиками. | 2 |
| **Тема 6. Система управління ризиками. Системи управління інциндентами.** Computer security and incident response team. Статистика. Міжнародний стандарт ITIL. Компоненти ITSM. Сфера використання ITSM. Принципи ITSM. Основні цілі процесів підтримки сервісів ITSM. Менеджмент інциндентів згідно стандарту ITIL. Основні етапи менеджменту інцідентів згідно стандарту ITIL. Топ 5 найбільших кіберзагрози у світі. Концепція побудування ефективної системи менеджменту інцидентів ІБ. Структура типічної автоматизованої системи менеджменту інцидентів ІБ. | 2 |
| **Тема 7. Захист персональніх даних.** Загальні поняття та визначення. Елементи інформаційних систем персональних даних. Класифікація загроз безпеки персональних даних. Склад елементів опису загроз НСД. Зовнішній порушник. Внутрішній порушник. Уразливості окремих протоколів стека протоколів TCP/IP. Загальна характеристика загроз НСД в операційному середовищі ІСПД. Загальна характеристика загроз на основі міжмережевої взаємодії. Етапи реалізації загрози. Нетрадиційні інформаційні канали. Соціальні мережі. | 2 |
| **Тема 8. Принципи захисту інформації при підключенні до Інтернету.** Еволюція кіберзагроз. Приклад цільової атаки. Смертельний ланцюг: після зараження. Відкриті системи ISO/OSI. Динаміка DDOS-атак по індустріям. Ампліфікація атаки. Скорочення часу на масовий злам. Модель загроз інформації для вузлу інтернет при проведенні типових видалених атак. Класифікація вірусів. Модель загроз інформації для вузла Інтернет при проведенні типових віддалених атак. Схема створення TCP-з'єднання. Схема реалізації атаки «нав'язування хибного маршруту» з використанням протоколу ICMP з метою перехвання трафіка. Схема реалізації атаки «впровадження хибного DNS-серверу» шляхом перехвату DNS-запросу. SQL-ін'єкція. Техніка CLICKJACKING. АТАКАARP-SPOOFING. Соціальна інженерія (social engineering). Механізм роботи антивірусів. | 2 |
| **Загальна кількість годин** | **16** |

## Лабораторні заняття

| Теми лабораторних занять | Кількість годин | Вагові коефіцієнти $a$ |
|---|---|---|
| **Тема 1. Порівняння даних за допомогою хешу.** Основні поняття хешування. Властивості хеш-функцій (стійкість, односторонність, рівномірність). Приклади популярних хеш-алгоритмів (MD5, SHA-2, SHA-3). Використання хешів для перевірки цілісності даних. Практичне застосування в інформаційній безпеці. | 3 | 0,1 |
| **Тема 2. Методи та шляхи збору та обробки інформації. Що було зроблено?.** | 3 | 0,1 |

| | | |
|---|---|---|
| Джерела збору інформації (відкриті, закриті, технічні). Методи збору: OSINT, SIGINT, HUMINT. Автоматизовані інструменти обробки інформації. Верифікація та перевірка достовірності даних. Приклади успішного використання зібраної інформації. | | |
| **Тема 3. Створення та збереження надійних паролей.** Вимоги до складності паролів. Менеджери паролів як засіб захисту. Методи атак на паролі (brute force, dictionary, rainbow tables). Багатофакторна автентифікація. Рекомендації щодо збереження паролів. | 3 | 0,1 |
| **Тема 4. Резервне копіювання даних до зовнішнього сховища.** Призначення та необхідність резервного копіювання. Типи резервного копіювання (повне, інкрементальне, диференційне). Використання хмарних та локальних сховищ. Методи шифрування резервних копій. Політика відновлення після інцидентів. | 3 | 0,1 |
| **Тема 5. Інформаційне протиборство. Хто володіє Вашими даними?** Сутність інформаційного протиборства. Роль держави, корпорацій та користувачів у збереженні даних. Методи збору персональних даних. Проблема приватності та цифрових слідів. Приклади реальних випадків витоку даних. | 3 | - |
| **Тема 6. Аналітичне забезпечення інформаційної безпеки. Дослідіть ризики своєї поведінки в Інтернеті (командна робота).** Методи аналізу ризиків в інформаційній безпеці. Види ризиків у поведінці користувача онлайн. Практичні інструменти моніторингу активності. Колективний аналіз прикладів небезпечної поведінки. Розробка рекомендацій для безпечного користування Інтернетом. | 3 | 0,1 |
| **Тема 7. Класифікація програмних та криптографічних засобів забезпечення інформаційної безпеки.** Програмні засоби захисту: антивіруси, міжмережеві екрани, IDS/IPS. Криптографічні засоби: симетричні та асиметричні алгоритми. Захист каналів передачі даних. Засоби управління ключами. Практичні приклади комплексних систем безпеки. | 3 | - |
| **Тема 8. Електронна ідентифікація користувачів. Нормативне забезпечення інформаційної безпеки. Загрози безпеки.** Методи електронної ідентифікації (паролі, токени, біометрія). Електронний підпис та його правове значення. Нормативно-правова база у сфері інформаційної безпеки. Основні кіберзагрози для електронної ідентифікації. Практика застосування в Україні та світі. | 3 | 0,1 |
| **Тема 9. Системна класифікація та характеристика технічних засобів забезпечення інформаційної безпеки.** Засоби контролю доступу (смарт-карти, біометрія). Системи запобігання вторгненням. Технічні засоби захисту каналів зв'язку. Системи резервного копіювання та відновлення. Приклади сучасних технічних засобів кіберзахисту. | 4 | 0,1 |
| **Тема 10. Міжнародні стандарти та рекомендації в галузі забезпечення інформаційної безпеки.** Основні міжнародні стандарти (ISO/IEC 27000, NIST, GDPR). Роль міжнародних організацій у забезпеченні безпеки. Методології управління інформаційною безпекою. Порівняння стандартів | 4 | 0,1 |

| | | |
|---|---|---|
| різних країн. Тенденції розвитку міжнародного регулювання кібербезпеки. | | |
| **Загальна кількість годин** | **32** | $\sum_{i=1}^{n} a_i$=0,8 |

## Контрольні роботи

| Теми контрольних робіт | Вагові коефіцієнти $b$ |
|---|---|
| **Тема 1. Захист інформації на рівні користувача та держави: методи, засоби, нормативне забезпечення.** Надійні паролі та багатофакторна автентифікація. Резервне копіювання та відновлення даних. Електронна ідентифікація та електронний підпис. Нормативно-правова база забезпечення інформаційної безпеки. | 0,1 |
| **Тема 2. Інформаційне протиборство та міжнародні стандарти безпеки.** Сутність інформаційного протиборства та його учасники. Методи збору та обробки інформації. Класифікація програмних, технічних та криптографічних засобів захисту. Міжнародні стандарти та рекомендації (ISO/IEC, NIST, GDPR). | 0,1 |
| **Загалом** | $\sum_{i=1}^{m} b_i$=0,2 |

## Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

## Опрацювання теоретичного матеріал

| Теми для самостійного вивчення | Кількість годин |
|---|---|
| **Тема 1. Методи створення та збереження надійних паролів.** Вимоги до складності сучасних паролів. Використання менеджерів паролів. Двофакторна та багатофакторна аутентифікація. Типові помилки користувачів при створенні паролів. | 11 |
| **Тема 2. Резервне копіювання та хмарні технології збереження даних.** Принципи резервного копіювання (повне, диференційне, інкрементальне). Хмарні сервіси (Google Drive, OneDrive, Dropbox) та їхні переваги/ризики. Локальні vs віддалені сховища. Захист резервних копій від несанкціонованого доступу. | 11 |
| **Тема 3. Сучасні загрози інформаційній безпеці держави та суспільства.** Кіберзлочинність та її вплив на національну безпеку. Кібершпигунство та кібератаки на критичну інфраструктуру. Соціальна інженерія як загроза. Роль держави у протидії кіберзагрозам. | 10 |
| **Тема 4. Інформаційне протиборство: сутність, приклади та наслідки.** Поняття інформаційної війни та її основні інструменти. Приклади інформаційних атак у світі та в Україні. Вплив фейкових новин і пропаганди на суспільну думку. Методи протидії інформаційним загрозам. | 10 |
| **Тема 5. Міжнародні стандарти у сфері інформаційної безпеки (ISO/IEC, NIST).** Основні стандарти ISO/IEC 27000-серії. Рекомендації NIST щодо управління ризиками. Європейські директиви та регламенти (GDPR, NIS Directive). Роль міжнародних організацій у формуванні політики безпеки. | 10 |
| **Тема 6. Програмні та криптографічні засоби захисту інформації.** | 10 |

| | |
|---|---|
| Антивірусні програми та системи виявлення вторгнень (IDS/IPS). Використання шифрування для захисту даних. Цифрові підписи та сертифікати. VPN-технології та захист трафіку. | |
| **Тема 7. Нормативно-правове забезпечення інформаційної безпеки в Україні.**<br>Конституційні положення щодо захисту інформації. Закон України «Про інформацію» та «Про кібербезпеку». Нормативно-правові акти щодо захисту персональних даних. Роль державних органів у забезпеченні інформаційної безпеки. | 10 |
| **Загальна кількість годин** | **72** |

## Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

### Рекомендовані курси, тренінги, стажування

1. Онлайн-курс CISCO «Cyber Ess»
https://www.netacad.com/catalogs/learn?category=course.

## Література, навчальні матеріали та інформаційні ресурси

### Основна література

1. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.
https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
2. Богуш В. М., Юдін О. К. Інформаційна безпека держави. - К.: "МК-Прес", 2005. - 432с.
3. Термінологічний довідник з питань технічної захисту інформації / Коженевський С.Р., Кузнєцов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. - К.: ДУІКТ, 2007. - 365 с.
4. Бобало Ю.Я., Горбатій І.В. (ред.) Інформаційна безпека. Навчальний посібник. - Львів: Видавництво Львівської політехніки, 2019. - 580 с. - ISBN 978-966-941-339-0.
https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.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.

### Додаткова література

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 31.12.2023. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 27.10.2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. Указ Президента України: Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ Президента України від 6 травня 2015 року № 287/2015. Дата оновлення: 16.09.2020. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text
4. Про національну безпеку: Закон України від 21.06.2018 № 2469-VIII. Дата оновлення: 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

5. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL: https://www.iso.org/ru/contents/data/standard/08/28/82875.html
6. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls URL: https://www.iso.org/ru/contents/data/standard/08/05/80585.html
7. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL: https://www.iso.org/ru/contents/data/standard/08/05/80585.html.
8. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

## Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників $k$:

| Поточний контроль (практичні, семінарські, лабораторні заняття), $k_1$ | Контрольні роботи (за наявності), $k_2$ | Індивідуальне завдання (за наявності), $k_3$ | Підсумковий контроль (для ОК з іспитом), $k_4$ |
|---|---|---|---|
| 0,8 | 0,2 | | |

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
$K$ – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: $a_i$ - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: $b_i$ - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, $K$, І,... ) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання

**Шкала оцінювання**

| Сума балів | Національна оцінка | ECTS |
|---|---|---|

знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

| | | |
|---|---|---|
| 90–100 | Відмінно | A |
| 82–89 | Добре | B |
| 75–81 | Добре | C |
| 64–74 | Задовільно | D |
| 60–63 | Задовільно | E |
| 35–59 | Незадовільно (потрібне додаткове вивчення) | FX |
| 1–34 | Незадовільно (потрібне повторне вивчення) | F |

## Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

## Погодження

| | | | |
|---|---|---|---|
| Силабус погоджено | 30.08.2025 | | **Завідувач кафедри**<br>Сергій ЄВСЕЄВ |
| | 30.08.2025 | | **Гарант ОП**<br>Сергій ЄВСЕЄВ |