Силабус освітнього компонента
Програма навчальної дисципліни

Основи математичного моделювання систем безпеки

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Обов'язкова

Семестр
5

Мова викладання
Українська

Викладачі, розробники

МІЛЕВСЬКИЙ Станіслав Валерійович
stanislav.milevskyi@khpi.edu.ua
кандидат економічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Науковий Гарант освітньо-наукової програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Основи математичного моделювання систем безпеки», «Англійська мова в академічних застосунках», «Моделювання кіберфізичних дій» у студентів бакалавріата та магістратури.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Основи математичного моделювання систем безпеки" є обов`язковою навчальною дисципліною. Дисципліна спрямована на придбання навичок в галузі моделювання систем, оволодіння методами імітаційного моделювання із застосуванням пакета (PowerSim).

Мета та цілі дисципліни

Формування у студентів теоретичних знань з основ моделювання систем безпеки, засвоєння студентами основних підходів і принципів побудови моделей та надбання навичок їх застосування для вирішення задач моделювання, що виникають при розробці інформаційних систем та систем безпеки.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
КЗ 2. Знання та розуміння предметної області та розуміння професії.
КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Результати навчання

РН–1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
РН–2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
РН–3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
РН–4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН–5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
РН–6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
РН–7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
РН–8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
РН–9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
РН–10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
РН–11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.

РН–12. Розробляти моделі загроз та порушника.
РН–13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
РН–14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
РН–15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
РН–16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
РН–17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
РН–18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН–19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
РН–20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
РН–21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН–22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН–23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН–24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
РН–25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
РН–26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
РН–27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
РН–28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
РН–29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
РН–30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
РН–31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
РН–32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

РН–33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
РН–34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН–35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН–36. Виявляти небезпечні сигнали технічних засобів.
РН–37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
РН–38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
РН–39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
РН–40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
РН–41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН–42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
РН–43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
РН–44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
РН–45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
РН–46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
РН–47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
РН–48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
РН–49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
РН–50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
РН–51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
РН–52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
РН–53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
РН–54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

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)

Вища математика, Основи побудови та захисту сучасних операційних систем, Математичні основи криптології.

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

Теми лекційних занять

Тема 1. Моделювання. Основні поняття. Види моделей, їх класифікація. Вимоги до моделей.
Поняття моделювання, поняття системи та моделі, основні типи моделей, види моделей та їх класифікація за різними критеріями, вимоги до моделей.
Тема 2. Основні види моделювання. Формальні методи побудови моделей.
Основні види моделювання (аналітичне, імітаційне, статистичне), їх характеристики та відношення між собою. Формальні методи побудови моделей: кібернетичний підхід, системна динаміка, теоретично-множинний підхід.
Тема 3. Ідентифікація параметрів математичної моделі. Адекватність, чутливість, непротирічність моделі.
Постановка завдання ідентифікації, основні етапи його вирішення та їх взаємозв’язок. Поняття адекватності, чутливості та непротирічності моделі, формальні способи їх перевірки.
Тема 4. Принципи побудови моделей. Технологія моделювання.
Основні принципи побудови моделей: інформаційної достатності, доцільності, здійсненності, множинності моделей, агрегації, параметризації, застосування методології ітераційного багаторівневого моделювання. Технологія моделювання: основні етапи, їх взаємозв'язок та характеристики.
Тема 5. Основні поняття і визначення, що використовуються при описі моделей безпеки комп'ютерних систем.
Елементи теорії комп'ютерної безпеки. Сутність, суб'єкт, доступ, інформаційний потік. Класична класифікація загроз безпеки інформації. Види інформаційних потоків. Види політик управління доступом та інформаційними потоками. Витік права доступу і порушення безпеки КС.
Математичні основи моделей безпеки. Основні поняття. Поняття автомата. Елементи теорії графів. Алгоритмічно розв'язні і алгоритмічно нерозв'язні проблеми. Модель решітки. Основні види формальних моделей безпеки. Проблема адекватності реалізації моделі безпеки в реальному комп'ютерній системі.
Тема 6. Моделі комп'ютерних систем з дискреційним управлінням доступом.
Модель матриці доступів Харрісона-Руззо-Ульмана. Опис моделі. Аналіз безпеки систем ХРУ. Модель типізованої матриці доступів. Модель поширення прав доступу Take-Grant. Основні положення класичної моделі Take-Grant. Розширена модель Take-Grant. Подання систем Take-Grant системами ХРУ. Дискреційні ДП-моделі. Базова ДП-модель. ДП-модель без кооперації довірених і недовірених суб'єктів.
Тема 7. Моделі ізольованого програмного середовища.
Суб'єктно-орієнтована модель ізольованого програмного середовища. Коректність суб'єктів в ДП-моделях КС з дискреційним управлінням доступом. ДП-модель з функціонально асоційованими з суб'єктами сутностями. ДП-модель для політики безпечного адміністрування. ДП-модель для політики абсолютного поділу адміністративних і призначених для користувача повноважень. ДП-модель з функціонально або параметрично асоційованими з суб'єктами сутностями. Застосування ФАС ДП-моделі для аналізу безпеки веб-систем. Методи запобігання витоку прав доступу і

реалізації заборонених інформаційних потоків. Метод запобігання можливості отримання права доступу володіння недовірених суб'єктом до довіреній суб'єкту. Метод реалізації політики безпечного адміністрування. Метод реалізації політики абсолютного поділу адміністративних і призначених для користувача повноважень.

Тема 8. Моделі комп'ютерних систем з мандатним управлінням доступом.

Модель Бела-ЛаПадули. Класична модель Бела-ЛаПадули. Приклад некоректного визначення властивостей безпеки. Політика low-watermark в моделі Бела-ЛаПадули. Приклади реалізації заборонених інформаційних потоків. Безпека переходів. Модель мандатної політики цілісності інформації Віба. Модель систем військових сполучень. Загальні положення та основні поняття. Неформальне опис моделі СВС. Формальний опис моделі СВС. Мандатна ДП-модель. Правила перетворення станів мандатної ДП-моделі. Безпека в сенсі Бела-ЛаПадули. Умови підвищення суб'єктом рівня доступу.

Тема 9. Моделі безпеки інформаційних потоків.

Автоматна модель безпеки інформаційних потоків. Програмна модель контролю інформаційних потоків. Імовірнісна модель безпеки інформаційних потоків. ДП-моделі безпеки інформаційних потоків за часом. ДП-модель з блокуючими доступами довірених суб'єктів. Мандатна ДП-модель з блокуючими доступами довірених суб'єктів. Мандатна ДП-модель з ототожненням породжених суб'єктів. Мандатна ДП-модель КС, що реалізують політику суворого мандатної управління доступом.

Тема 10. Моделі комп'ютерних систем з рольовим управлінням доступом.

Поняття рольового управління доступом. Базова модель рольового управління доступом. Модель адміністрування рольового управління доступом. Основні положення. Адміністрування множин авторизованих ролей користувачів. Адміністрування множин прав доступу, якими володіють ролі. Адміністрування ієрархії ролей. Модель мандатної рольового управління доступом. Захист від загрози конфіденційності інформації. Захист від загроз конфіденційності та цілісності інформації. Мандатна сутнісно-рольова ДП-модель управління доступом та інформаційними потоками в операційних системах сімейства Linux. Стан системи. Функціонально або параметрично асоційовані суті. Доступи і права доступу. Завдання мандатної управління доступом для станів системи. Завдання мандатної контролю цілісності для станів системи. Фактичне володіння. Правила перетворення станів.

Тема 11. Моделі взаємодії в кібербезпеці.

Модель Лотка-Вольтерра. Класифікація типів взаємодій. Конкуренція. Хижак-жертва. Модель Колмогорова.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Автоматні моделі. Модель мережі Петрі.
Тема 2. Моделі системної динаміки.
Тема 3. Дискретно-часові моделі.
Тема 4. Структурні моделі безпеки.
Тема 5. Імітаційні моделі.
Тема 6. Моделювання комп'ютерних систем з дискреційним управлінням доступом.
Тема 7. Моделі ізольованого програмного середовища.
Тема 8. Моделі комп'ютерних систем з мандатним управлінням доступом.
Тема 9. Моделі безпеки інформаційних потоків.
Тема 10. Моделі комп'ютерних систем з рольовим управлінням доступом.
Тема 11. Моделі систем взаємодії.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

Основна література:

1. Бахрушин В.Є. Математичне моделювання: навчальний посібник [Текст] – Запоріжжя: ГУ "ЗІДМУ", 2004. – 140 с.
http://moodle.nati.org.ua/mod/resource/view.php?id=7442
2. Жерновий Ю. В. Імітаційне моделювання систем масового обслуговування : Практикум / Ю. В. Жерновий. — Львів : Вид. центр ЛНУ ім. І. Франка, 2007. — 307 с.
https://new.mmf.lnu.edu.ua/wp-content/uploads/2018/02/Imit_model.pdf
3. Математичне моделювання систем і процесів: навч. посібник / П. М. Павленко, С. Ф. Філоненко, О. М. Чередніков, В. В. Трейтяк. – К. : НАУ, 2017. – 392 с.
https://pdf.lib.vntu.edu.ua/books/2020/Pavlenko_2017_392.pdf
4. Математичне моделювання телекомунікаційних систем та мереж: навчальний посібник [Текст] / Є.М. Чернихівський. – Львів: Видавництво Львівської політехніки, 2011. – 272 с.
https://vlp.com.ua/node/7158
5. Махней О. В. Математичне моделювання : навчальний посібник / О. В. Махней. — Івано-Франківськ : Супрун В. П., 2015. — 372 с.
https://kdrpm.pnu.edu.ua/wp-content/uploads/sites/55/2018/03/matmod_content.pdf
6. Томашевський В.М. Моделювання систем / В.М. Томашевський. — К. : Видавнича група BHV, 2005. — 352 с.
https://pdf.lib.vntu.edu.ua/books/2016/Tomashev_2005_352.pdf
7. 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
8. 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
9. 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.

Додаткова література :

10. Махней О. В. Математичне забезпечення автоматизації прикладних досліджень / О. В. Махней, Т. П. Гой. — Івано-Франківськ : Сімик, 2013. — 304 с.
https://kdrpm.pnu.edu.ua/wp-content/uploads/sites/55/2018/03/Maple_content.pdf
11. Павленко П. М. Основи математичного моделювання систем і процесів:навч. посіб. – К.: Книжкове вид-во НАУ, 2013. – 201 с.
https://er.nau.edu.ua/bitstream/NAU/24750/1/%D0%A2_%D0%9F%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9F.%D0%9C._%D0%9D%D0%B0%D0%B2%D1%87.pdf

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% семестрової оцінки;
•іспит: 40% семестрової оцінки

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
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

Студент 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

28.08.2024 Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024 Гарант ОП
Сергій ЄВСЕЄВ