Силабус освітнього компонента
Програма навчальної дисципліни

Інноваційне підприємництво та управління стартап проєктами

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

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

Освітня програма
Освітньо-наукова програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Загальна підготовка, Обов'язкова

Семестр
2

Мова викладання
Українська

Викладачі, розробники

ХВОСТЕНКО Владислав Сергійович

vladyslav.khvostenko@khpi.edu.ua
Кандидат економічних наук, доцент кафедри кібербезпека НТУ «ХПІ».

Автор більше 30 публікацій: з них 3 монографії у співавторстві 1 посібник з грифом. Провідний лектор з дисциплін: «Інтелектуальна власність систем безпеки», «Правове регулювання кібербезпеки».
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна «Інноваційне підприємництво та управління стартап проектами» передбачає вивчення та розвиток стартап культури та підприємницьких навичок у студентів, що є критично важливою складовою створенням ефективної системи розвитку інноваційного підприємництва в Україні.

Мета та цілі дисципліни

Формування системи знань і практичних навичок у створенні і управлінні стартапами на початковій стадії, підготовка студентів до участі в інкубаційних, акселераційних і грантових програмах підтримки стартапів.

Формат занять

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

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КЗ–4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та

використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ11. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій..

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 16 год., практичні роботи – 16 год., самостійна робота – 58 год.

Передумови вивчення дисципліни (пререквізити)

Безпека систем Клієнт-Сервер.

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.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Стартап екосистема.
Особливості інноваційного підприємництва. Що таке стартап. Стадії розвитку стартапу. Стартап екосистема. Гравці та їх ролі. Огляд стартап екосистеми України та найвідоміших стартапів.
Тема 2. Основні принципи формування команди, ролі в команді стартапу.
Що таке команда. Команда vs Група. Принципи формування команди. Ролі в команді. Цінності, місія та візія команди.
Тема 3. Дизайн мислення. Визначення проблем, емпатія.
Вступ до ДМ. 5 основних блоків. Задача VS Ідея. Кейс стаді. AirBnb, IKEA family. Стадія емпатії. Методи побудови емпатії. Карта емпатії. Стадія визначення проблеми. «How might we»|| питання.
Тема 4. Дизайн мислення. Пошук і вибір.
Стадія генерування ідеї. Методи та інструменти. Відбір ідей. Брейнстормінг та як з ним працювати.
Тема 5. Валідація ідеї стартапу.
Формування краш-тест ідей, які команди обрали собі для подальшої роботи на стартапом. Валідація ідеї через цей краш-тест, пошук слабких сторін.
Тема 6. Канва бізнес моделі. Вступ, проблема та рішення.
Що таке бізнес модель, для чого вона потрібна. Види бізнес моделей. Огляд складових Lean Canvas.
Тема 7. Канва бізнес моделі. Портрет клієнта, ціннісна пропозиція.
Визначення терміну customer development. Сегментація клієнтів. Клієнт vs Користувач. B2B, B2C, B2G. Створення портрету клієнтів. Канва ціннісної пропозиції.
Тема 8. Дослідження клієнтів. Попереднє дослідження ринку. Валідація ключових гіпотез.
Цикл customer development. Гіпотези. Валідація гіпотез. Інструменти для проведення дослідження клієнтів - опитувальники, інтерв'ю, фокус групи. Дослідження трендів та статистичних даних. Платформи Kickstarter, Product Hunt та ін.
Тема 9. Презентації ідей стартапів.
Презентування напрацювань команд. Валідувати ідеї команд та результати кастдеву.
Тема 10. Динаміка команди.
Динаміка команди. Етапи розвитку команди. Методи роботи з командою на різних етапах, мотивація. Проєктний менеджмент.
Тема 11. Мінімальний життєздатний продукт.
Що таке MVP. Задачі, характеристики. Інструменти та стадії створення MVP. Огляд кейсів AirBnB, Dropbox.
Тема 12. Оцінка ринку. Аналіз конкурентів. Нечесні конкуренті переваги.
Поняття об'єму ринку. Методи оцінки ринку. Аналіз росту ринку. TAM, SAM, SOM. Методи аналізу конкурентів. Складові. Нечесні конкурентні переваги (unfair advantages).
Тема 13. Основи маркетингу для стартапів.
Маркетингова стратегія для стартапу. Основи цифрового маркетингу. SMM та інструменти онлайн просування. Реклама, робота з лідерами думки. Метрики.
Тема 14. Основи про інвестиції, фінанси та юридичні особливості стартапів.
Типи інвесторів та інвестицій. Етапи та раунди інвестицій. Юридичні аспекти інвестицій.
Тема 15. Презентація стартапу. Пітч-дек.
Теоретичні засади підготовки презентацій. Правила успішного пітчингу. Розбір прикладів наповнення слайдів та структури презентації різних відомих стартапів.

Теми практичних занять

Тема 1. Правила складання і подання заявки на винахід та заявки на корисну модель.
Тема 2. Здійснення формальної експертизи заяви на винахід. Державні збори та мита.
Тема 3. Контроль складання та подання заявки на промисловий зразок.
Тема 4. Вирішення практичних завдань із правозастосовчих заходів на митному кордоні.
Тема 5. Вирішення практичних завдань із захисту авторського і суміжних прав.
Тема 6. Вирішення практичних завдань із захисту прав на торговельні марки.
Тема 7. Вирішення практичних завдань із захисту прав на винаходи.
Тема 8. Вирішення практичних завдань із захисту прав на комерційну таємницю.

Теми лабораторних робіт

Лабораторні роботи в рамках дисципліни не передбачені.

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.
Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:
Launching a Business Venture, Managing a Business Venture
https://www.netacad.com/catalogs/learn?category=course.

Література та навчальні матеріали

Основна література

1. Котлубай В. О. Інноваційне підприємництво та управління стартап проектами. Economic evaluation of innovative solution : практикум / В. О. Котлубай, Г. А. Отливанська. – Одеса : НУ "ОЮА", 2021. – 131 с. [Електронний ресурс]. – Режим доступу: https://dspace.onua.edu.ua/server/api/core/bitstreams/dbd21a89-cc80-479b-9f28-17b4d8998767/content
2. Ден Сенор, Сол Синґер. Країна стартапів. Історія ізраїльського економічного дива. Yakaboo Publishing. 2016. – 368 с. [Електронний ресурс]. – Режим доступу: https://findbook.in.ua/books/krayina-startapiv-istoriia-izrayil-s-kogho-iekonomichnogho-diva
3. Гавриш О. А., Бояринова К. О., Копішинська К. О. Розробка стартап-проектів: практикум [Електронний ресурс]: навч. посіб. для студ. спеціальностей 151 – «Автоматизація та комп'ютерно-інтегровані технології» та 152 – «Метрологія та інформаційно-вимірювальна техніка». Електронні текстові данні (1 файл: X,XX Мбайт). Київ : КПІ ім. Ігоря Сікорського, 2019. 116 с. [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/a1ad390a-6a4b-40b2-944f-e82dc7f8e3db/content
4. Гавриш О. А., Бояринова К. О., Копішинська К. О. Розробка стартап-проектів: Конспект лекцій [Електронний ресурс]: навч. посіб. для студ. спеціальностей 151 – «Автоматизація та комп'ютерно-інтегровані технології» та 152 – «Метрологія та інформаційно-вимірювальна техніка». Електронні текстові данні (1 файл: X,XX Мбайт). Київ: КПІ ім. Ігоря Сікорського, 2019. – 188 с. [Електронний ресурс]. – Режим доступу:

https://ela.kpi.ua/server/api/core/bitstreams/63391483-0014-435b-866f-ab3188b5a372/content
5. Шаповал В.А. Опорний конспект лекцій «Стартап міжнародних проектів» для студентів спеціальності «076 19 Підприємництво, торгівля та біржова діяльність». Дніпро: ДВНЗ «НГУ», 2017. – 29 с. [Електронний ресурс]. – Режим доступу: https://pe.nmu.org.ua/ua/studentam/magistr/076/mb/%D0%9A%D0%9B_%D0%A1%D0%90%D0%9C%D0%9F.pdf
6. Тимур Ворона. Стартап на мільйон: як українці заробляють статки на технологіях. – К. : Видавництво «ВІВАТ», 2017. – 224 с.
7. Ли Галлахер. Історія Airbnb: Як троє звичайних хлопців підірвали готельну індустрію. – К. : Видавництво: "Book Chef", 2018. [Електронний ресурс]. – Режим доступу: https://www.google.com.ua/books/edition/Airbnb_%D0%9A%D0%B0%D0%BA_%D1%82%D1%80%D0%B8_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%8B%D1%85_%D0%BF%D0%B0/AK5VDwAAQBAJ?hl=ru&gbpv=1&dq=%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F+Airbnb:+%D0%AF%D0%BA+%D1%82%D1%80%D0%BE%D1%94+%D0%B7%D0%B2%D0%B8%D1%87%D0%B0%D0%B9%D0%BD%D0%B8%D1%85+%D1%85%D0%BB%D0%BE%D0%BF%D1%86%D1%96%D0%B2+%D0%BF%D1%96%D0%B4%D1%96%D1%80%D0%B2%D0%B0%D0%BB%D0%B8+%D0%B3%D0%BE%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%83+%D1%96%D0%BD%D0%B4%D1%83%D1%81%D1%82%D1%80%D1%96%D1%8E.&printsec=frontcover

Додаткова література

1 Бен Горовіц. Безжальна правда про нещадний бізнес. Розбудова бізнесу в умовах невизначеності. – К. : Видавництво «Наш формат», 2015. – 264 с. [Електронний ресурс]. – Режим доступу: https://chtyvo.org.ua/authors/Horovits_Ben/Bezzhalna_pravda_pro_neschadnyi_biznes_Rozbudova_biznesu_v_umovakh_nevyznachenosti/
2. Боб Дорф, Стів Бланк. Священна книга стартапера. Як збудувати успішну компанію. – К. : Видавництво «Наш формат», 2018. – 512 с. [Електронний ресурс]. – Режим доступу: https://www.yakaboo.ua/ua/svjaschenna-kniga-startapera-jak-zbuduvati-uspishnu-kompaniju.html
3. Олександр Остервальдер, Ів Піньє. Створюємо бізнес-модель. – К. : Видавництво «Наш формат», 2017. – 228 с. [Електронний ресурс]. – Режим доступу: https://www.google.com.ua/books/edition/%D0%A1%D1%82%D0%B2%D0%BE%D1%80%D1%8E%D1%94%D0%BC%D0%BE_%D0%B1%D1%96%D0%B7%D0%BD%D0%B5%D1%81_%D0%BC%D0%BE%D0%B4%D0%B5/HXiYDwAAQBAJ?hl=ru&gbpv=1&dq=%D0%9E%D0%BB%D0%B5%D0%BA%D1%81%D0%B0%D0%BD%D0%B4%D1%80+%D0%9E%D1%81%D1%82%D0%B5%D1%80%D0%B2%D0%B0%D0%BB%D1%8C%D0%B4%D0%B5%D1%80,+%D0%86%D0%B2+%D0%9F%D1%96%D0%BD%D1%8C%D1%94.+%D0%A1%D1%82%D0%B2%D0%BE%D1%80%D1%8E%D1%94%D0%BC%D0%BE+%D0%B1%D1%96%D0%B7%D0%BD%D0%B5%D1%81-%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C.+%E2%80%93+%D0%9A.+:+%D0%92%D0%B8%D0%B4%D0%B0%D0%B2%D0%BD%D0%B8%D1%86%D1%82%D0%B2%D0%BE+%C2%AB%D0%9D%D0%B0%D1%88+%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%C2%BB,+2017.+%E2%80%93+228+%D1%81&printsec=frontcover

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•практичні роботи: 50% 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
Ольга КОРОЛЬ