Силабус освітнього компонента
Програма навчальної дисципліни

Управління IT-проектами та їх безпека

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
Профільна підготовка, Вибіркова

Семестр
7

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

В межах дисципліни «Управління IT-проектами та їх безпека» формуються теоретичні знання в сфері управління проектами; визначаються особливості використання сучасного програмного забезпечення для успішного управляння проектом. Вивченню дисципліни «Управління IT-проектами та їх безпека» передують дисципліни: «Теорія алгоритмів та програмування», «Об'єктно-орієнтоване проектування та моделювання», «Системний аналіз», «Технології програмного забезпечення». Дисципліна «Управління IT-проектами та їх безпека» може служити підготовчою базою для виконання кваліфікаційної роботи бакалавра.

Мета та цілі дисципліни

Вивчення методів та інструментів області управляння проектами, а також отримання компетентностей, необхідних для визначення та успішного досягнення цілей проектів з розробки програмного забезпечення шляхом керування обсягом робіт, ресурсами, часом, якістю, ризиками та змінами.

Формат занять

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

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
КЗ 6. 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.
КЗ 7. 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.
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 їх 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 кредита ECTS): лекції – 32 год., лабораторні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Алгоритми та структури даних, Технології програмування, Основи програмування.

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 лекції-візуалізації (презентації), пояснення, демонстрування, виконання завдань лабораторних робіт. Контрольні заходи: захист лабораторних робіт, опитування, тестування

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Загальна характеристика управління проектами програмного забезпечення.
Класифікація базових понять і типів проектів. Життєвий цикл проекту. Структуризація проекту. Мета, стратегія і результат проекту. Ризики проекту.
Тема 2. Основи мережевого і календарного планування проекту. Планування ресурсів та витрат проекту.
Системний підхід до проектування виробництва й управління проектами. Мережеві моделі. Аналіз структурного різноманіття складних проектів.
Тема 3. Методологія управління IT проектами
Інструкція зі складання проекту. Основні методи управління. Загальний план проекту. Структура розбиття робіт (WBS). Відповідальні віхи.
Тема 4. Форми організаційної структури проекту. Поняття критичного шляху.
Метод критичного шляху. Розрахунок резервів часу . Графік Ганта. Призначення і використання. Метод оцінки та перегляду планів (Перт). Мережевий графік: «робота в вузлі».
Тема 5. Інформаційні технології управління проектами .
Загальна характеристика програмного забезпечення проектів. Огляд деяких найбільш доступних програмних систем планування проектів. Засоби збору даних, розподілу інформації та підтримки групової роботи.
Тема 6. Планування бюджету проекту. Оцінка ефективності проекту.
Управління вартістю проекту. Управління часом, задумом, якістю, людськими ресурсами, комунікаціями проекту.
Тема 7. Управління ризиками в проектах. Контроль виконання проекту.
Управління забезпеченням проекту. Принципи кількісного управління. Управління ризиками проекту.
Тема 8. Управління командою і комунікаціями проекту програмного забезпечення.
Відстеження проекту. Формування звітності.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Розробка моделі проекту в середовищі OpenProj. Діаграма Ганта. Характеристики проекту. Завдання. Віхи.
Тема 2. Методи дослідження проектних ситуацій.
Тема 3. Створення зв'язків. Встановлення обмежень.
Тема 4. Ресурсне планування проекту. Призначення ресурсів
Тема 5. Обчислення критичного шляху.
Тема 6. Вирівнювання ресурсів проекту. Створення базового плану
Тема 7. Ризики проекту. Принципи кількісного управління.
Тема 8. Відстеження проекту. Формування звітності.

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:
Managing a Business Venture
https://www.netacad.com/catalogs/learn?category=course.

Література та навчальні матеріали

Основна література:

1. Буріменко Ю. І., Галан Л. В., Лебедєва І. Ю., Щуровська А. Ю. Управління проєктами : навч. посібник. Одеса : ОНАЗ ім. О. С. Попова, 2017. 208 с.
https://h.twirpx.link/file/3935278/.
2. Довгань Л.Є., Мохонько Г.А., Малик І.П. Управління проєктами : навч. посібник. Київ : КПІ ім. Ігоря Сікорського, 2017. 420 с.
https://ela.kpi.ua/server/api/core/bitstreams/cf735d19-339f-44c8-8b5a-42f40468edf4/content.
3. Ноздріна Л., Ящук В., Полотай О. Управління проєктами. Київ : Центр навчальної літератури, 2010. 432 с.
http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/UpravlinnyaProektamiNozdrina2010.pdf.
4. Хігні Д. Основи управління проєктами. Харків : Фабула, 2020. 272 с.
https://elib.chdtu.edu.ua/e-books/4229.
5. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). Seventh Edition : Project Management Institute, 2021. 250 p.
https://ibimone.com/PMBOK%207th%20Edition%20(iBIMOne.com).pdf.
6. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
http://kist.ntu.edu.ua/textPhD/tzi.pdf.

Додаткова література :

7. Зачко О. Б., Івануса А.І., Кобилкін Д.С. Управління проектами: теорія, практика, інформаційні технології. – Львів: ЛДУ БЖД, 2019. – 173 с.

https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/9721/1/%D0%9A%D0%BD%D0%B8%D0%B3%D0%B0%20%D0%A3%D0%9F.pdf
8. Блага Н. В. Управління проєктами : навч. посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 152 с.
https://dspace.lvduvs.edu.ua/bitstream/1234567890/3870/1/%D0%B1%D0%BB%D0%B0%D0%B3%D0%B0%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F%20%D0%BF%D1%80%D0%BE%D1%94%D0%BA%D1%82%D0%B0%D0%BC%D0%B8.pdf
9. Яковенко О.І. Управління проєктами та ризиками : навч. посібник. Ніжин : Видавець ПП Лисенко М.М., 2019. 196 с.
http://dspace.idgu.edu.ua/jspui/bitstream/123456789/830/1/%D0%AF%D0%9A%D0%9E%D0%92%D0%95%D0%9D%D0%9A%D0%9E%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F%20%D0%BF%D1%80%D0%BE%D0%B5%D0%BA%D1%82%D0%B0%D0%BC%D0%B8%20%D1%82%D0%B0%20%D1%80%D0%B8%D0%B7%D0%B8%D0%BA%D0%B0%D0%BC%D0%B8.pdf
10. Cicala G. The Project Managers Guide to Microsoft Project 2019. Apress, 2020. 681 p.
https://www.abebooks.com/9781484256374/Project-Managers-Guide-Microsoft-2019-1484256379/plp
11. Dionisio C.S. Microsoft Project 2019 For Dummies John Willey & Sons, Inc., 2019. 352 p.
https://books.google.com.ua/books/about/Microsoft_Project_2019_For_Dummies.html?id=JymFDwAAQBAJ&redir_esc=y
12. Kerzner H. Project Management: A Systems Approach to Planning, Scheduling, and Controlling, 12th Edition. John Willey & Sons, Inc., 2017. 848 p.
https://books.google.com.ua/books/about/Project_Management.html?id=xlASDgAAQBAJ&redir_esc=y
13. Євсеєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсеєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с.
http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/Yevseiev.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;
- залік: 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

Гарант ОП

28.08.2024

Сергій ЄВСЕЄВ