



Силабус освітнього компонента

Програма навчальної дисципліни



Управління IT-проектами та їх безпека

Шифр та назва спеціальності

257– Управління інформаційною безпекою

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Освітня програма

Управління інформаційною безпекою

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 кібербезпеки 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 управління 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 управління 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 реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

КЗ-2. 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.

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-4. Здатність спілкуватися державною мовою як усно, так і письмово.

КЗ-5. Здатність спілкуватися іноземною мовою.

КЗ-6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.

КЗ-8. Здатність до соціальної взаємодії, співробітництва, розв'язання конфліктів у сфері професійної діяльності, лідерства і командної роботи.

ФК-1. Здатність використовувати безпекові режими під час виконання службових обов'язків.

ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.

ФК-4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.

ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.

ФК-6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.

ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.

ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

ФК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.

ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.

ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

ПРН-1. Вміти реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства (вільного демократичного) та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

ПРН-2. Вміти використовувати 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.

ПРН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.

ПРН-4. Вільно спілкуватися державною мовою.

ПРН-5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.

ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.

ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.

ПРН-9. Вміти використовувати безпекові режими під час виконання службових обов'язків.

ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

ПРН-11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.

ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.

ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

ПРН-15. Вміти визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки.

ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

ПРН-17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

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., Лебедева І. Ю., Щуровська А. Ю. Управління проектами : 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 проектами : 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 проектами. Київ : Центр навчальної літератури, 2010. 432 с.
http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/UpravlinnyaProektamiNozdrina2010.pdf.
4. Хігні Д. Основи управління проектами. 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](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 проектами : 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 проектами 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 Wiley & Sons, Inc., 2019. 352 p.
[https://books.google.com.ua/books/about/Microsoft Project 2019 For Dummies.html?id=JymFDwAAQBAJ&redir_esc=y](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 Wiley & Sons, Inc., 2017. 848 p.
[https://books.google.com.ua/books/about/Project Management.html?id=xIASDgAAQBAJ&redir_esc=y](https://books.google.com.ua/books/about/Project+Management.html?id=xIASDgAAQBAJ&redir_esc=y)
13. Євсєєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПТОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсєєв, 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 ВСЕЄВ

28.08.2024



Гарант ОП

Роман КОРОЛЬОВ