Силабус освітнього компонента
Програма навчальної дисципліни

«Ризик-орієнтований аналіз в IT-технології»

Шифр та назва спеціальності
123 – Комп’ютерна інженерія

Інститут
ННІ Комп'ютерних наук та інформаційних технологій

Освітня програма
Сучасне програмування, мобільні пристрої та комп’ютерні ігри (інноваційний кампус)

Кафедра
Комп’ютерна інженерія та програмування (326)

Рівень освіти
Бакалавр

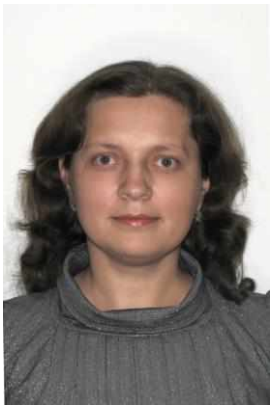
Тип дисципліни
Профільна підготовка
Вільний вибір студента

Семестр
7

Мова викладання
Українська, англійська

Викладачі, розробники

Бельорін-Еррера Олександра Михайлівна,
e-mail: bellher@ukr.net;
старший викладач, кандидат педагогічних наук
Основні курси: «Ризик-орієнтований аналіз в IT-технології», «Дискретна математика» (практ.), «Вступ до спеціальності. Основи комп'ютерної інженерії» (практ.).
Детальніше про викладача на сайті кафедри: https://web.kpi.kharkov.ua/cep/2022/10/03/belorin-errera-oleksandra-myhajlivna/.



Мнушка Оксана Василівна
e-mail: mnushka.ov@gmail.com;
старший викладач.
Основні курси: «Програмування» (англ., практ., лаб.), «Основи комп’ютерної математики» (англ.), «Розробка та застосування баз даних» (англ.), «Ризик-орієнтований аналіз в IT-технології» (англ.).
Детальніше про викладача на сайті кафедри: https://web.kpi.kharkov.ua/cep/2022/10/03/mnushka-oksana-vasylivna/.

Загальна інформація

Анотація

«Ризик-орієнтований аналіз в IT-технології» один з курсів профільної підготовки, що продовжує фундаментальну підготовку бакалаврів за освітньою програмою – «Сучасне програмування, мобільні пристрої та комп'ютерні ігри (інноваційний кампус)». Вона формує фахівця за освітньою кваліфікацією бакалавра з комп'ютерної інженерії. Освітня компонента передбачає здатність володіння фахівцями сучасними методами аналізу IT-ризиків та розробки ефективного процесу управління IT-ризиками.

Мета та цілі дисципліни

Розвиток системного мислення, надання студентам основних знань з теоретичних і практичних основ аналізу та ефективного управління IT-ризиками а також формування відповідних умінь та компетентностей.

Формат занять

Лекції та практичні заняття, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

ФК9. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.
ФК 13. Здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій.

Результати навчання

ПРН 1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

ПРН 2. Мати навички проведення експериментів, збирання даних та моделювання в комп'ютерних системах.

ПРН 9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

Обсяг дисципліни

Загальний обсяг дисципліни 120 (3 кредитів ECTS): лекції –24 год., практичні заняття – 24 годин, самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Для успішного проходження курсу необхідно знати: основи безпеки програм та даних, основи комп'ютерної інженерії.

Особливості дисципліни, методи та технології навчання

Лекції проводяться інтерактивно з використанням мультимедійних технологій. На практичних заняттях використовується проєктний підхід до навчання та ігрові методи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Поняття IT- ризику.
Мета та задачі дисципліни. Категорії IT-ризиків. Види ризиків в IT-системах.

Тема 2. Методика оцінки IT-ризиків.
Якісна оцінка IT- ризиків. Кількісна оцінка IT- ризиків. Тріада CAI.

Тема 3. Процес управління IT-ризиками.
Етапи процесу управління IT-ризиками. Контроль IT-ризиків. Зменшення IT-ризиків.

Тема 4. Стандарти управління IT-безпекою.
Що таке стандарт? Політика України в галузі стандартизації. Міжнародні стандарти щодо управління ризиками ISO. NIST. COSO ERM.

Тема 5. Політика управління IT-ризиками.
Процедури безпеки IT, стандарти, політика IT-персоналу.

Тема6. Реагування на IT-інциденти та відновлення.
План реагування на IT-інциденти. Планування відновлення IT-інцидентів

Тема 7. Програмне забезпечення щодо управління ризиками.
Програмне забезпечення для управління ризиками підприємства (ERM). Управління, управління ризиками та відповідність (GRC). Інтегроване управління ризиками (IRM).

Тема 8. Загальний регламент захисту даних «GDPR».
Принципи захисту даних відповідно до GDPR. Інформація про конфіденційність відповідно до GDPR. Принцип безпеки відповідно до GDPR.

Теми практичних занять

Тема 1. Ідентифікація ризику
Побудова причинно-наслідкову діаграма для ризиків IT-проекту.

Тема 2. Якісна оцінка ризику
Побудова матриці наслідків і ймовірностей. Заповнення реєстру ризиків IT-проекту.

Тема 3. Кількісна оцінка ризиків.
Розрахунок ALE.

Тема 4. Експертна оцінка ризиків.
Розрахування коефіцієнт конкордації. Визначення ступінь узгодженості думок експертів.

Тема 5. Аудит IT-інфраструктури.
Складання звіту із зазначенням всіх виявлених помилок та недоліків у роботі IT-системи, а також рекомендаціями щодо її вдосконалення.

Тема 6. Моделювання загроз безпеки.
Побудова дерева атак.

Тема 7. Оцінка ризиків за допомогою Microsoft Security Assessment Tool
Оцінки ризиків організації, пов'язаних з інформаційною безпекою, з використанням ПЗ Microsoft Security Assessment Tool (MSAT).

Тема 8. Аналіз звітів MSAT.
Аналіз результатів звіту MSAT щодо оцінки безпеки підприємства.

Теми лабораторних робіт

Не передбачені.

Самостійна робота

Самостійна робота є основним засобом оволодіння здобувачем навчального матеріалу та включає: опрацювання теоретичного матеріалу та самопідготовку до лекційних, практичних занять; підготовку до усного опитування або тестування. Студентам також рекомендуються додаткові матеріали (відео, статті, підручники) для самостійного вивчення та аналізу.

Література та навчальні матеріали

Основна література:

1. IT Risk Management. [Online]. Available at: https://www.nibusinessinfo.co.uk/content/it-risk-management.

2. Кравченко, М.О., Бояринова, К.О., Копішинська, К.О. (2021). Управління ризиками: Навчальний наочний посібник [Risk Management: An Educational Visual Guide]. КПІ ім. Ігоря Сікорського. Available at: https://ela.kpi.ua/bitstream/123456789/43528/1/

3. Бельорін-Еррера, О.М., Кучук, Н.Г., Лисиця, О.Х. (2024). Методичні вказівки до виконання практичних занять з дисципліни "Ризик-орієнтований аналіз в IT-технології" для студентів денної та заочної форми навчання за спеціальністю 123 "Комп'ютерна інженерія" . НТУ "ХПІ".

4. Бельорін-Еррера, О.М. (2024). Ризик-орієнтований аналіз в IT-технології. Конспект лекцій [НТУ "ХПІ".

5. Cyber Security for Business. [Online]. Available at: https://www.nibusinessinfo.co.uk/content/cyber-security-business.

6. CISA Resources & Tools. [Online]. Available at: https://www.cisa.gov/resources.

7. ISACA IT Risk Management Resources. [Online]. Available at: https://www.isaca.org/resources/it-risk.

8. Free Online Course: Risk Management and Resource Evaluation from Alison. [Online]. Available at: https://alison.com/course/risk-management.

9. NIST Risk Management Framework. [Online]. Available at: https://csrc.nist.gov/projects/risk-management.

10. How to Make a Risk Management Plan (Template Included) from ProjectManager.com. [Online]. Available at: https://www.projectmanager.com/blog/risk-management-plan-template.

11. Gerunov, A.A. (2023) Risk analysis for the Digital age. Cham: Springer Nature.

12. Modarres, M. and Groth, K. (2023) Reliability and risk analysis. Boca Raton, FL: CRC Press, an imprint of the Taylor & Francis Group.

13. Stamatis, D.H. (2019) Risk management using failure mode and effect analysis (FMEA). Milwaukee, WI: ASQ Quality Press.

14. Liu, H.-C. (2016) FMEA using uncertainty theories and MCDM methods. Singapore: Springer Singapore, Imprint: Springer.

.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

100% підсумкової оцінки складаються з результатів оцінювання у вигляді екзамену (40%) та поточного оцінювання (60%).
Екзамен: письмове завдання (2 запитання з теорії + розв'язання задачі) та усна доповідь.
Поточне оцінювання: 2 онлайн теста (20%), практичні заняття (40%)

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	Дата погодження, підпис 22.04.2024	Завідувач кафедри Олександр ЗАКОВОРОТНИЙ
	Дата погодження, підпис 22.04.2024	Гарант ОП Олександр ЗАКОВОРОТНИЙ