Силабус освітнього компонента
Програма навчальної дисципліни

Моделювання систем критичної інфраструктури

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
3

Мова викладання
Українська

Викладачі, розробники

АКСЬОНОВА Ірина Вікторівна

Iryna.Aksonova@khpi.edu.ua
Кандидат економічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 150, з них свідоцтв на авторський твір - більше 15, розділів у монографіях - 10, статей, що реферуються у науково метричних базах Scopus та WoS - 9. Лектор з дисциплін: "Моделювання інформаційних систем", "Штучний інтелект і бізнес-аналітика", "Стандартизація та сертифікація в галузі інформаційної безпеки", "Технологія управління безпекою бізнес-процесів" та інших у студентів бакалавріата та магістратури.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Моделювання систем критичної інфраструктури" є обов'язковою навчальною дисципліною. Актуальність даної дисципліни для фахівця з безпеки обумовлюється тим, що моделювання – це найефективніший спосіб дослідження складних систем різного призначення, як на етапі їх проектування, так і в процесі експлуатації.

Мета та цілі дисципліни

Метою дисципліни є формування у студентів теоретичних та практичних знань, вмінь та навичок щодо методології і принципів дослідження, проектування, підтримки функціонування та науково-технічного супроводження критичних об’єктів та критичних інфраструктур. Вивчення дисципіни сприяє отриманню практичних навичок по системному аналізу критичних систем, формалізації математичних моделей та алгоритмів прийняття рішень, які використовуються при дослідженні безпеки критичних систем та інфраструктур.

Формат занять

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

Компетентності

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.
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-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
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-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-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-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-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 інфораційною 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-мунікаційних 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 кредити ECTS): лекції – 32 год., лабораторні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Технології 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 презентації, бесіди.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Методологічні основи моделювання систем критичної інфраструктури.
Тема 2. Методи збору інформації та даних про систему і побудова моделей.
Тема 3. Формалізація процесів функціонування дискретних систем.
Тема 4. Аналітичне багатовимірне моделювання.
Тема 5. Імітаційне моделювання систем критичної інфраструктури.
Тема 6. Методи дослідження та оптимізації моделей.
Тема 7. Методи самоорганізації моделей.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Методи та процес моделювання.
Тема 2. Визначення закону розподілу в первинній інформації щодо систем критичної інфраструктури.
Тема 3. Визначення функціональної залежності між складовими системи.
Тема 4. Побудова функціональної моделі IDEF0.
Тема 5. Моделі системи засобами мереж масового обслуговування та мереж "Петрі".
Тема 6. Методи багатовимірного моделювання та їх застосування в досліджені систем критичної інфраструктури.
Тема 7. Аналітичне моделювання систем критичної інфраструктури.
Тема 8. Експериментальні методи пошуку оптимальних значень.
Тема 9. Алгоритми самоорганізації моделей.

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. Харченко В.С., Яковлев С.В., Горбачик О,С. та ін. Забезпечення функціональної безпеки критичних інформаційно–керуючих систем : монографія/ за ред. В.С.Харченка, С.В.Яковлева. Харків: Константа,2019. 272 с.
2. Математичне моделювання інформаційних систем: навчальний посібник / І. І. Обод, І. В. Свид, І. В. Рубан, Г. Е. Заволодько. Харків : Друкарня Мадрид, 2019. 270 с.
https://repository.kpi.kharkov.ua/server/api/core/bitstreams/fb92b600-f702-4d8e-b27f-6df6040fe8c4/content
3. Моделювання та оптимізація систем: підручник /Дубовой В. М., Квєтний Р. Н., Михальов О. І., А.В.Усов А. В. Вінниця : ПП «ТД«Еднльвейс», 2017. 804 с.
https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/19937/Modeluvannia_ta_optymizatsiia_system.pdf?sequence=1&isAllowed=y
4. Великодний С. С. Моделювання систем: конспект лекцій. Одеський державний екологічний університет, 2018. 186 с.
http://eprints.library.odeku.edu.ua/708/1/VelykodniySS_Modelirovanie_system_KL_2018.pdf
5. Гороховатський В.О., Творошенко І.С. Методи інтелектуального аналізу та оброблення даних: навч. посібник. Харків: ХНУРЕ, 2021. 92 с.
https://openarchive.nure.ua/server/api/core/bitstreams/2e55d639-52fd-48d9-b7b7-14989f49f291/content

Додаткова література :

1. Казакова Н. Ф., Штефан Н. З. Методичні вказівки до виконання лабораторних робіт (частина 1) з навчальної дисципліни «Системний аналіз і проектування інформаційних систем» для студентів денної та дистанційної форми навчання напрямку – «комп'ютерні науки». ОДЕкУ, 2022, 109 с.
http://eprints.library.odeku.edu.ua/10727/2/Kazakova_Shtefan_Sys_analysis_Proekt_IS.pdf
2. Основи теорії інформаційних систем : Лабораторний практикум для студентів напряму 6.050101 «Комп'ютерні науки» / уклад.: І.Е. Райчев, О.Г. Харченко. Київ: Видав. Нац. авіац. ун-ту ―НАУ-друк‖, 2015. 48 с.
https://core.ac.uk/download/pdf/323013267.pdf
3. Клен К. С. Методи моделювання інформаційних систем: навчальний посібник. Київ. КПІ ім. Ігоря Сікорського, 2023. 193 с.
https://ela.kpi.ua/server/api/core/bitstreams/6453589e-1ae8-438e-b385-1873b7635464/content
4. Лабораторний практикум з використанням STATISTICA та EXCEL / Вільчинська О.М. Львів: ЛНУ ім. Івана Франка, 2017. 80 с.
https://econom.lnu.edu.ua/wp-content/uploads/2016/09/Model-i-prohnoz.pdf
5. Кузьмичов А. І. Оптимізаційні методи і моделі. Моделювання засобами MS Excel // навчальний посібник. Київ: Видавництво Ліра-К, 2017. 215 с.
https://profbook.com.ua/index.php?route=product/product/download&product_id=6902&download_id=2134

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

28.08.2024

Гарант ОП
Роман КОРОЛЬОВ