Кам'янець-Подільський національний університет імені Івана Огієнка Фізико-математичний факультет
Кафедра комп'ютерних наук

СИЛАБУС ДИСЦИПЛІНИ

«Системи захисту об'єктів критичної інфраструктури»

122 Комп'ютерні науки, 014 Середня освіта (Математика), 014 Середня освіта (Фізика) [ОКР «магістр», 2 семестр, 2022-2023 н. р.]

Інформація про викладачів

Викладач

Слободянюк Олександр Васильович,

Контактні дані викладача

Адреса: 32300, вул. Симона Петлюри 1, каб. 24
Email: slobodyanyuk@ieee.org
Роб. тел. +38 03849 31601
кандидат технічних наук, доцент

Загальна інформація про курс

Мова викладання

Українська

Опис

Дисципліна має на меті познайомити слухачів із методами та засобами захисту об'єктів критичної інфраструктури. Дисципліна спрямована на формування у студентів практичних навичок й теоретичних знань про об'єкти критичної інфраструктури та попередження порушень у сфері життєзабезпечення населення. Крім того метою даної дисципліни є формувань поняття об'єктів критичної інфраструктури, їх видів та співвідношення з нормальною життєдіяльністю державних служб та громадян.

Курс «Системи захисту об'єктів критичної інфраструктури» належить до дисциплін професійної підготовки.

Тип дисципліни: вибіркова.

Мета та завдання курсу

Метою дисципліни «Системи захисту об'єктів критичної інфраструктури» є формування теоретичних знань іта практичних навичок, необхідних для аналізу характеристик, оцінки ефективності та використання систем захисту об'єктів критичної інфраструктури.

Основні завдання вивчення дисципліни "Системи захисту об'єктів критичної інфраструктури" полягають у тому, щоб дати студентів розуміння основних понять критичних систем, що складаються з окремих секторів та елементів, які безпосередньо взаємопов'язані, навчити їх практичному застосуванню цих систем для розв'язання конкретних задач захисту інформації критичних систем; ознайомити з сучасними способами захисту критичних інфраструктур, відомими підходами до аналізу загроз та ризиків, тенденціями розвитку систем, навчити їх методам синтезу й аналізу критичних систем.

Формат курсу

Стандартний очний навчальний курс.

Очікувані результати навчання (з урахуванням soft skills)

Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.

Використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв’язання задач теоретичного та прикладного характеру в процесі проектування та реалізації об’єктів інформатизації.

Здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності програмного забезпечення.

6. Очікувані результати навчання з дисципліни.

Оцінювати та забезпечувати якість інформаційних та комп'ютерних систем різного призначення.

Тестувати програмне забезпечення.

Виконувати дослідження у сфері комп'ютерних наук.

Виявляти та усувати проблемні ситуації в процесі експлуатації програмного забезпечення, формулювати завдання для його модифікації або реінжинірингу

Сторінки курсу у LMS

Moodle: https://moodle.kpnu.edu.ua/course/view.php?id=7729

Аудиторія, години консультацій

Корпус №3, каб. 29. Щочетверга, 15:00-16:00

Зміст курсу

Обсяг курсу

Кількість кредитів ЄКТС: 4
Загальний обсяг годин: 120 год
Кількість годин навчальних занять: 40 год
Лекційні заняття: 12 год
Практичні заняття: 28 год

Структура курсу

К-ть акад. год.	Тема заняття	Форма заняття	Матеріали	Завдання	Вага оцінки (балів)	Термін виконання
2	Тема 1. Поняття критичної інфраструктури	Лекція	Презентація	Ознайомитись із рекомендовано ю літературою	Не оцінюється	Відповідно навчального розкладу факультету
4	Тема 2. Аналіз загроз для об'єктів критичної інфраструктури	Лекція	Презентація	Ознайомитись із рекомендованою літературою	Не оцінюється	Відповідно навчального розкладу факультету
2	Тема 3. Підхід деяких країн ЄС та США до критичних систем. Світовий досвід в організації критичних систем	Лекція	Презентація	Ознайомитись із рекомендованою літературою	Не оцінюється	Відповідно навчального розкладу факультету
2	Тема 4. Структура критичних систем	Лекція	Презентація	Ознайомитись із рекомендовано ю літературою	Не оцінюється	Відповідно навчального розкладу факультету
2	Тема 5. Система фізичного захисту критичних систем.	Лекція	Презентація	Ознайомитись із рекомендованою літературою	Не оцінюється	Відповідно навчального розкладу факультету
4	Дослідження ризиків.	Лабораторна робота	Методичні рекомендаціїна сторінках курсу у LMS	Виконати усі завдання, що запропоновані у методичних рекомендаціях	Робота студентів на навчальних заняттях, а також виконувані ними завдання оцінюються за 12-бальною шкалою	За п'ять днів до дати проведення семестрового екзамену

К-ть акад. год.	Тема заняття	Форма заняття	Матеріали	Завдання	Вага оцінки (балів)	Термін виконання
4	Дослідження загроз.	Лабораторна робота	Методичні рекомендаціїна сторінках курсу у LMS	Виконати усі завдання, що запропоновані у методичних рекомендаціях	Робота студентів на навчальних заняттях, а також виконувані нимизавдання оцінюються за 12-бальною шкалою	За п'ять днів до дати проведення семестрового екзамену
8	Дослідження системи захисту критичних систем.	Лабораторна робота	Методичні рекомендаціїна сторінках курсу у LMS	Виконати усі завдання, що запропоновані у методичних рекомендаціях	Робота студентів на навчальних заняттях, а також виконувані нимизавдання оцінюються за 12-бальною шкалою	За п'ять днів до дати проведення семестрового екзамену
4	Дослідження системи фізичного захисту критичних систем	Лабораторна робота	Методичні рекомендаціїна сторінках курсу у LMS	Виконати усі завдання, що запропоновані у методичних рекомендаціях	Робота студентів на навчальних заняттях, а також виконувані нимизавдання оцінюються за 12-бальною шкалою	За п'ять днів до дати проведення семестрового екзамену
8	Розробка системи захисту	Лабораторна робота	Методичні рекомендаціїна сторінках курсу у LMS	Виконати усі завдання, що запропоновані у методичних рекомендаціях	Робота студентів на навчальних заняттях, а також виконувані нимизавдання оцінюються за 12-бальною шкалою	За п'ять днів до дати проведення семестрового екзамену

Політики курсу

Вимоги дисципліни: обов'язкове відвідування аудиторних занять, попередня підготовка до лекцій і лабораторних занять з методичних вказівок і основної літератури, якісне і своєчасне виконання завдань самостійної роботи, участь у всіх видах контролю (поточний контроль, контроль самостійної роботи студента, підсумковий контроль). Якщо Ви без запізнень відвідайте всі заняття, будете активно працювати на заняттях, виконаєте всі завдання якісно і в строк, то наберете максимальний бал, зазначений в календарному графіку контрольних заходів. Поважні причини пропуску занять не звільняють студента від виконання всього комплексу практичних, лабораторних і самостійних робіт. В цьому випадку Вам надається можливість відпрацювати його по індивідуальним завданням і в час, вказаний викладачем.

Академічна доброчесність. Роботи студентів повинні бути оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.

Пререквізити курсу (Prerequisites)

Теоретичною базою вивчення дисципліни «Системи захисту об’єктів критичної інфраструктури» є попередні навчальні дисципліни: «Сучасні технології програмування», «Сучасні операційні системи, та ін.

Постреквізити (Postrequisites)

Знання і вміння, які отриманні під час вивчення дисципліни «Системи захисту об’єктів критичної інфраструктури» використовуються при вивченні дисциплін «Управління IT-проектами», «Тестування програмних систем», «Інтелектуальні інформаційні системи».

Система оцінювання та вимоги

Курс даної навчальної дисципліни складається з 1-го навчального (змістового) модуля. Для оцінювання знань, умінь та навичок студентів в кожному змістовому модулі передбачається проведення поточного контролю на лабораторних заняттях, який проводиться у вигляді захисту результатів роботи.

Поточний контроль полягає в перевірці теоретичних знань та практичних умінь і навичок під час лабораторних та практичних занять. Максимальний бал оцінки поточної успішності студентів на лабораторних заняттях приймається рівним 12. Критерії оцінювання знань, умінь, навичок і фахових компетенцій студентів на навчальних заняттях наведено в таблиці:

1	Студент мало усвідомлює мету завдання; може відшукати відповідь у підручнику лише на окремі питання.
2	Студент слабо володіє понятійним апаратом; відповідає лише за допомогою викладача на рівні “так” чи “ні”; може самостійно знайти в підручнику відповідь.
3	Студент володіє навчальним матеріалом на рівні засвоєння окремих термінів, фактів без зв’язку між ними; робить спроби виконання вправ, дій репродуктивного характеру за допомогою викладача.
4	Студент володіє початковими знаннями, здатний відтворити їх, провести за ними розрахунки з допомогою викладача; самостійне опрацювання навчального матеріалу викликає значні труднощі.
5	Студент знає більше половини навчального матеріалу, розуміє сутність навчальної дисципліни, може дати визначення понять (однак з помилками); вміє працює з підручником; робить прості розрахунки за алгоритмом, але висновки не логічні, не послідовні.
6	Студент розуміє основні положення навчального матеріалу, може поверхнево аналізувати суть завдання, робить певні висновки; відповідь може бути правильною, проте недостатньо осмисленою; самостійно відтворює більшу частину матеріалу; вміє застосовувати знання під час розв’язування розрахункових завдань з алгоритмом.
7	Студент правильно і логічно відтворює навчальний матеріал, оперує базовими поняттями і фактами, встановлює причинно-наслідкові зв’язки між ними; правильно використовує термінологію; вміє наводити приклади на підтвердження своїх думок; здатний за допомогою викладача застосовувати знання в стандартних ситуаціях.
8	Знання студента досить повні; відповіді чіткі, логічні та обґрунтовані, однак з окремими неточностями; вміє самостійно проаналізувати хід розв’язання задачі і на її прикладі розв’язати аналогічну.
9	Студент вільно володіє вивченим матеріалом; вміє аналізувати і систематизувати інформацію, робити висновки; використовує загальновідомі докази у власній аргументації; вміє самостійно працювати; без сторонньої допомоги виконує прості завдання, здатний розв’язувати складні задачі, використовуючи приклади аналогічних задач, розв’язаних до нього.
10	Студент володіє узагальненими знаннями з дисципліни, аргументовано використовує їх у стандартних ситуаціях; чітко тлумачить поняття, формулює закони; може самостійно опрацьовувати матеріал; має сформовані типові навички; здатний самостійно розв’язати стандартну задачу; робить спроби застосовувати знання у дещо змінених ситуаціях.
11	Студент володіє глибокими і міцними знаннями; дає правильні і вичерпні відповіді, робить аргументовані висновки; здатний самостійно вивчити матеріал; самостійно визначає шлях розв’язання стандартних задач; здатний розв’язувати складні нестандартні завдання, використовуючи попередні навідні підказки.
12	Студент має системні теоретичні знання, аргументовано застосовує їх при розв’язанні практичних завдань; знає суміжні дисципліни; ґрунтовно й логічно викладає матеріал в усній та письмовій формі; самостійно вибирає шлях розв’язання задачі (в тому числі складної, нестандартної) та доводить його до кінця, використовує широкий арсенал засобів для обґрунтування та доведення своєї думки; схильний до системнонаукового аналізу та прогнозування результатів, моделює ситуації в нестандартних умовах.

Пропущені студентом заняття обов’язково відпрацьовуються. Поточну заборгованість (оцінки 0, 1, 2, 3), пов’язану з не підготовкою (недостатньою підготовкою) до занять студент також повинен ліквідувати. При цьому максимальним балом за відпрацьоване заняття вважається 12.

Рейтингова оцінка у балах поточної успішності студента з навчального (змістового) модуля обчислюється після проведення усіх занять модуля та ліквідації студентом поточної заборгованості за такою формулою:

$$r_k = \left(0{,}05 \times r_k^c + 0{,}4\right) \times \hat{r}_k ,$$

де r_k^c – середня оцінка навчальної діяльності студента на навчальних заняттях, а $\hat{r}_k$ – встановлений максимально можливий бал оцінювання результатів поточної успішності студента за змістовий модуль.

Підсумковий рейтинг з кредитного модуля виставляється відповідно до таблиці:

Рейтингова оцінка з кредитного модуля	Оцінка за шкалою ECTS	Рекомендовані системою ECTS статистичні значення (у %)	Екзаменаційна оцінка за національною шкалою	Національна залікова оцінка
90-100 і більше	A (відмінно)	10	відмінно	зараховано
82-89	B (дуже добре)	25	добре	
75-81	C (добре)	30		
67-74	D (задовільно)	25	задовільно	
60-66	E (достатньо)	10		
35-59	FX (незадовільно з можливістю повторного складання)		незадовільно	не зараховано
34 і менше	F (незадовільно з обов'язковим проведенням додаткової роботи щодо вивчення навчального матеріалу кредитного модуля)			

На основі всього вище зазначеного наведемо таблицю, в якій вказані бали для кожного виду діяльності в рамках модулів:

СЕМЕСТР 3

Поточний контроль (100 балів)	Залік
Модуль 1 (100 балів)	**100**
Поточний контроль	
100 балів	

Рекомендована література.

Основна:

1) Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання. URL: https://jurkniga.ua/contents/derzhavna-sistema-zakhistu-kritichnoi-infrastrukturi-ukraini-kontseptualni-zasadi-administrativno-pravovogo-regulyuvannya.pdf
2) Посібник з європейського права у сфері захисту персональних даних URL: https://rm.coe.int/16805966a8
3) Навчальний посібник основи управління інформаційною безпекою. URL:URL:https://er.dduvs.in.ua/bitstream/123456789/5717/1/ПОСІБНИК%20ОУІБ%20.pdf
3) Зелена книга з питань захисту критичної інфраструктури в Україні https://niss.gov.ua/sites/default/files/2014-11/1125_zelknuga.pdf с.
4) Хорошко В.О. Основи інформаційної безпеки / В.О. Хорошко, В.С. Чередниченко, М.Є: URL: https://duikt.edu.ua/ua/lib/4/category/729/view/1365
5) Hofreiter, L. a kol. (2013): Ochrana objektov kritickej dopravnej infrastruktury, Zilinsk? univerzita v Ziline/EDIS, Zilina. URL: http://fbiw.uniza.sk/kritinf/aktuality/publik/075_hofreiter_a_kol(ookdi-2013).pdf

Допоміжна:

1) Вакалюк Т.А. Захист інформації в комп'ютерних системах. Навчально-методичний посібник для студентів: URL: http://eprints.zu.edu.ua/9650/1/1.pdf
2) Технології захисту інформації : навчальний посібник. [Електронний ресурс] / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. URL: http://kist.ntu.edu.ua/textPhD/tzi.pdf
3) COM(2005) 576 final: Green paper: On a European Programme for Critical Infrastructure Protection, Brussels, 17.11.2005. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576

Інформаційні джерела

1) Закон України "Про державну таємницю". URL: https://zakon.rada.gov.ua/laws/show/3855-12
2) Закон України "Про захист інформації в автоматизованих системах". URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
3) Закон України "Про захист інформації в автоматизованих системах". URL: https://zakon.rada.gov.ua/laws/show/2594-15.
4) Закон України "Про інформацію". URL: https://zakon.rada.gov.ua/laws/show/2657-12

5) Закон України "Про науково-технічну інформацію". URL: https://zakon.rada.gov.ua/laws/show/3322-12
6) Закон України " Про електронні комунікації". URL: https://zakon.rada.gov.ua/laws/show/1089-20
7) Постанова Кабінет Міністрів України "Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію". URL: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF
8) Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. URL: https://tzi.ua/assets/files/НД-ТЗІ-2.5-005--99.pdf
9) НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi
10) НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi
11) Положення про порядок здійснення криптографічного захисту інформації в Україні. URL: https://zakon.rada.gov.ua/laws/show/505/98
12) Положення про технічний захист інформації в Україні. URL: https://zakon.rada.gov.ua/laws/show/1229/99

Сторінки курсу у LMS Moodle: https://moodle.kpnu.edu.ua/enrol/index.php?id=7729