Силабус освітнього компонента
Програма навчальної дисципліни

Управління інформаційною безпекою

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

Кафедра
Комп’ютерна інженерія та програмування (326)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Вибіркова

Семестр
7

Мова викладання
Українська

Викладачі, розробники

Поворознюк Оксана Анатоліївна

Oksana.Povorozniuk@khpi.edu.ua
Кандидат технічних наук, доцент кафедри «КІП» НТУ «ХПІ»

Автор понад 80 наукових та науково-методичних праць. Провідний лектор з дисциплін: «Управління інформаційною безпекою», «Основи наукових досліджень», «Computer architecture» та «Signal and Image Processing».
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Дисципліна спрямована на розгляд широкого кола питань щодо принципів створення комплексних систем захисту інформації (КСЗІ) в інформаційно – телекомунікаційних системах (ІТС), здійснення комплексу заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують обробку інформації в ІТС згідно з вимогами, встановленими нормативно – правовими документами у сфері захисту інформації.

Мета та цілі дисципліни

Забезпечення теоретичної підготовки для дослідження стану інформаційної безпеки комп'ютерних систем і мереж, надання знань про сучасні технології створення комплексних систем захисту інформації, отримання знань та навичок практичного застосування прийомів та методів захисту інформації в інформаційно-телекомунікаційних системах різного призначення.

Формат занять

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

Компетентності

ФК4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки;
ФК10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

Результати навчання

ПРН 8. Вміти системно мислити та застосовувати творчі здібності до формування принципово нових ідей.
ПРН 11. Вміти здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредитів ECTS): лекції – 32 год., практичні заняття – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Для успішного проходження курсу необхідно мати знання та практичні навички з наступних дисциплін: «Вища математика», «Алгебра програмування», «Програмування», «Теорія ймовірності», «Фізика» достатніх для:
- дослідження процесів збереження, накопичення, перетворення, передачі даних та інформації із застосуванням комп'ютерної техніки;
- вивчення методів створення комплексних систем захисту інформації;
- вивчення взаємодії в комп'ютерних мережах;
- вивчення методів вимірювання ризиків;
- дослідження технічних каналів витоку інформації.

Особливості дисципліни, методи та технології навчання

На лекційних заняттях викладання матеріалу здійснюється в усній формі із демонстрацією презентацій. Методи навчання: лекція-бесіда, лекція-візуалізація, навчальна дискусія, мозкова атака, кейс-метод, метод порівняння, метод узагальнення, метод конкретизації, метод відокремлення основного, обговорення, робота над помилками.
На практичних заняттях студенти виконують та демонструють індивідуальні завдання.
Під час самостійної роботи вдома студенти коректують свої індивідуальні завдання а також вивчають теми та питання, які не викладаються на лекційних заняттях.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Інформаційна безпека. Основні поняття та визначення
1.1 Вступ. Предмет курсу та його задачі. Структура, зміст дисципліни, його зв`язок з іншими дисциплінами та місце у підготовці інженера даного фаху.
1.2 Складові частини національної безпеки України. Система забезпечення інформаційної безпеки України. Нормативні документи. Основні поняття та визначення. Базові властивості інформації. Методи доступу до інформації.
1.3 Забезпечення безпеки. Класифікація загроз інформаційній безпеці. Структура та складові комплексної системи захисту інформації. Класифікація автоматизованого систем. Етапи розробки КСЗІ.
Тема 2. Принципи створення КСЗІ.
2.1 Обстеження ІТС та підготовка базових даних для формування вимог до КСЗІ. Елементи обстеження ІТС. Обстеження інформаційного середовища

2.2 Аналіз ризиків інформаційної безпеки, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін. Розробка моделі загроз та моделі порушника.
2.3 Розробка політики безпеки інформації в ІТС. Принципи розробки ПБ в ІТС. Об'єкти захисту. Етапи розробки політики безпеки. Методологія розробки політики безпеки
2.4 Структура концепції інформаційної безпеки компанії. Структура критеріїв захищеності інформації: критерії конфіденційності, критерії цілісності, критерії доступності, критерії спостереженості та критерії гарантій.

Тема 3. Основні напрямки та методи забезпечення безпеки інформації.

3.1 Вимоги до КСЗІ. Розробка функціонального профілю захищеності - перелік мінімально необхідних рівнів послуг, які повинна реалізувати КСЗІ. Семантика профілю. Стандартні профілі та рекомендації щодо їх використання. Служба захисту інформації, структура та функції.
3.2 Створення КСЗІ. Розробка ТЗ на створення КСЗІ. Розробка проекту КСЗІ. Вимоги та зміст проектної документації: ескізний проект, технічний проект, робочий проект. Робоча та експлуатаційна документація.

Тема 4. Методологія управління інформаційною безпекою.

4.1 Введення КСЗІ в дію та оцінка захищеності інформації в ІТС. Призначення та зміст етапів розробки КСЗІ: попередні випробування, дослідна експлуатація, державна експертиза, супроводження КСЗІ.
4.2 Концептуальна модель системи безпеки компанії. Управління ризиками. Аудит інформаційної безпеки. Практичні кроки аудиту інформаційної безпеки.
4.3 Управління ризиками. Технології аналізу та методи вимірювання ризиків. Вимірювання ризику при якісних величинах. Інструментальні засоби аналізу ризиків.
4.4 Технічні засоби і методи захисту інформації. Технічні канали витоку інформації. Засоби виявлення каналів витоку інформації Активні та пасивні методи та системи захисту інформації.

Тема 5. Методи та засоби забезпечення інформаційної безпеки.

5.1 Принципи криптографічного захисту інформації. Симетричні та асиметричні криптографічні системи. Ефективність захисту.Генерація ключів та обмін ключами. Електронний цифровий підпис і функція хешування.
5.2 Антивірусний захист. Класифікація комп'ютерних вірусів та програмних закладок. Файлові та бутові віруси, мережеві «черв'яки», «троянський кінь». Принципи побудови антивірусних програм.
5.3 Захист операційних систем та програмного забезпечення. Засоби активного та пасивного захисту. Електронні ключі. Технологія захисту інформації на основі смарт-карт. Створення захищеної операційної системи.
5.4 Безпечна взаємодія в комп'ютерних мережах. Типи атак в КМ. Захист КМ за допомогою сканерів та аналізаторів протоколів. Міжмережеві екрани. Фільтрація трафіка. Управління криптографічними ключами.

Теми практичних занять

Тема 1. Проектування системи фізичного захисту об'єкту. Дослідження принципів роботи охоронних систем на базі пасивних інфрачервоних датчиків руху і СВЧ датчиків руху.
Розробка проекту системи фізичного захисту об'єкту із застосуванням пасивних інфрачервоних датчиків руху і СВЧ датчиків руху згідно з інд. завданням.

Тема 2. Розробка моделі загроз та моделі порушника

Розробка моделі загроз та моделі порушника згідно з інд. завданням.

Тема 3. Розробка функціонального профілю захищеності та технічного завдання на створення КСЗІ

Розробка ТЗ на створення КСЗІ згідно з інд. завданням.

Тема 4. Управління інформаційними ризиками. Розрахунок рівня ризиків

Розрахунок рівня ризиків згідно з інд. завданням

Тема 5. Дослідження технічних засобів (приладів) і методів захисту інформації

Ознайомлення з системою технічного захисту згідно індивідуального завдання. Розрахунок можливості витоку інформації за рахунок побічних електромагнітних випромінювань (ПЕМВН)

Тема 6. Канали витоку акустичної та візуально-оптичної інформації. Розрахунок дальності розвідувального контакту акустичних та візуально-оптичних приладів

Розрахунок рівня акустичного сигналу та відстані контрольованої зони, необхідної для запобігання прослуховування мовної інформації за допомогою технічних приладів. Розрахунок дальності розвідувального контакту візуально– оптичних приладів.

Тема 7. Криптографічний захист інформації. Шифрування/розшифрування

Ознайомлення з алгоритмами криптографічного захисту. Виконання шифрування та розшифрування певної інформації згідно з інд. завданням, використовуючи відповідний алгоритм.

Тема 8. Захист операційних систем та програмного забезпечення. Дослідження захисних функцій ОС Windows

Виконання певних функцій адміністрування щодо захисту операційної системи згідно з інд. завданням. Дослідження захисних функцій ОС Windows, налаштування Брандмауера Windows.

Теми лабораторних робіт

Лабораторні роботи в рамках дисципліни не передбачені.

Самостійна робота

Опрацьовування лекційного матеріалу.
Підготовка до практичних занять та модульних контролів.
Самостійне вивчення тем та питань, які не викладаються на лекційних заняттях: нормативні документи у сфері інформаційної безпеки, дослідження принципів роботи охоронних систем, розробка концептуальної моделі інформаційної безпеки організації, вивчення природи виникнення побічних електромагнітних випромінювань (ПЕМВН), розглядання прикладів алгоритмів криптографічного захисту, функціонування брандмауера Windows, налаштування та робота з антивірусною програмою.

Література та навчальні матеріали

Основна література

1. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.
URL: https://knushop.com.ua/index.php?route=product/product&product_id=413
2. Управління інформаційною безпекою: навчально-методичний посібник./ А. І. Поворознюк, О.А. Поворознюк – Харків: НТУ «ХПІ», 2021. – 135 с.
URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/70560
3. Поворознюк А.І., Поворознюк О.А. Управління інформаційною безпекою: методичні вказівки до виконання практичних занять Харків: НТУ «ХПІ» -2022. – 123 с.
URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/70559
4. Писарчук О.О. Захист інформації в комп'ютерних системах»: Навч. посібник [Електронний ресурс] / Писарчук О.О.–Електронні текстові дані – Київ : КПІ ім. Ігоря Сікорського, 2020. – 95 с. Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № 6 від 31.01.2020 р.) за поданням Вченої ради ФІОТ (протокол № 4 від 25.11.2019 р.)
https://ela.kpi.ua/handle/123456789/48296
5. Поворознюк О.А. Багатокритеріальна оцінка альтернатив при проєктуванні двохфакторної автентифікації суб'єктів-користувачів в системах захисту інформації / А.І. Поворознюк, О.А. Поворознюк, Г.Є. Філатова // Системи управління, навігації та зв'язку, 2021 – вип. 2(64) – С.92-95.
URL: https://repository.kpi.kharkov.ua/items/4657763d-dda7-4908-9768-8b188576670c
URL: https://doi.org/10.26906/SUNZ.2021.2.092
6. Управління інформаційною безпекою. Конспект лекцій: навчальний посібник для студентів спеціальності 125 «Кібербезпека» / С. О. Носок, О. М. Фаль, В. М. Ткач. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.
URL: https://ela.kpi.ua/handle/123456789/43377
7. Методи та засоби технічного захисту інформації: навч. посіб. / В. М. Луценко, Д. О. Прогонов – Київ : КПІ ім. Ігоря Сікорського, 2021. – 289 с.
URL: https://ela.kpi.ua/handle/123456789/42397

8. Т.І. Каткова. Забезпечення криптографічного захисту державних інформаційних ресурсів // Міжвузівський збірник «Наукові нотатки». Луцьк, 2022, No73, С.54- 58
URL: https://doi.org/10.36910/775.24153966.2022.73.7
9. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
https://learn.ztu.edu.ua/pluginfile.php/264055/mod_resource/content/1/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%B8%20%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97_%D0%9D%D0%90%D0%92%D0%A7%D0%90%D0%9B%D0%AC%D0%9D%D0%98%D0%99_%D0%9F%D0%9E%D0%A1%D0%86%D0%91%D0%9D%D0%98%D0%9A.pdf

Додаткова література.

1. Закон України “Про інформацію” від 02.10.1992 року.
2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31.05.2005р., №2594- IV, К., 2005.
3. Про заходи щодо захисту інформаційних ресурсів держави. Затверджено Указом Президенту України №582 від 10.04 2000 року
4. Постанова КМУ від 29.03.2006р. № 373 « Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах ».
5. Порядок проведення робіт із створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. НД ТЗІ 3.1-003-2005.

Інформаційні ресурси в інтернеті.

Тематичні бази даних https://ufn.ru/en/articles.
Закордонні електронні наукові інформаційні ресурси: European Library. Вільний доступ до ресурсів 47 Національних бібліотек Європи, Австралії, Білорусії, Великої Британії, Німеччини, бібліотека коледжу Лондонського університету.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:
модульні контролі - 20 балів; практичні заняття - 60 балів; екзамен - 20 балів.

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	Завідувач кафедри Олександр ЗАКОВОРОТНИЙ
	Дата погодження, підпис	Гарант ОП Микола ЗАПОЛОВСЬКИЙ