Силабус освітнього компонента
Програма навчальної дисципліни

Апаратні засоби захисту інформації

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)

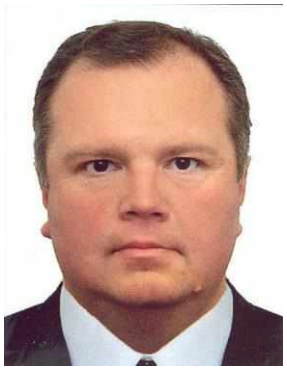
Рівень освіти
Бакалавр

Тип дисципліни
Професійна – Вибіркова

Семестр
7

Мова викладання
Українська, англійська

Викладачі, розробники



Главчев Максим Ігорович
Smaksym.glavchev@khpi.edu.ua
кандидат економічних наук, доцент, професор кафедри комп’ютерної інженерії та програмування НТУ «ХПІ»
Досвід роботи понад 30 років. Має більше 100 публікацій. Провідний лектор з дисциплін: «Апаратні засоби захисту інформації», «Програмні засоби захисту інформації», «Проєктування програм діагностики комп'ютерних систем та мереж», «Спеціалізовані комп'ютерні системи»
.
Детальніше про викладача на сайті кафедри
https://web.kpi.kharkov.ua/cep/2021/09/03/glavchev-maksym-igorovych/

Загальна інформація

Анотація

Апаратні засоби захисту інформаційних систем — засоби захисту інформації та інформаційних систем, реалізованих на апаратному рівні. Дані засоби є необхідною частиною безпеки інформаційної системи, це різноманітні за принципом дії, побудовою і можливостями конструкції, що забезпечують припинення розголошення, захист від витоку і протидію несанкціонованому доступу до джерел конфіденційної інформації.

Мета та цілі дисципліни

Мета навчальної дисципліни “ Апаратні засоби захисту інформації” забезпечити отримання відомостей про сучасні технології захисту інформації та цілеспрямоване їх використання для організації безпеки комп‘ютерних систем і мереж, для отримання знань та навичок практичного

використання методів та алгоритмів захисту інформації, надання знань про особливості проектування систем захисту та компонентів забезпечення безпеки інформації, принципи побудови комплексу апаратно-програмного забезпечення захисту, методи і засоби контролю та тестування окремих складових та системи безпеки в цілому.

Формат занять

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

Компетентності

ФК 4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки
ФК 8. Готовність брати участь у роботах з впровадження комп'ютерних систем та мереж, введення їх до експлуатації на об'єктах різного призначення.
ФК 10.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 1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.
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.
ПРН 11. Вміти здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Для успішного проходження курсу необхідно знати: програмування, системне програмування, архітектуру комп'ютерів, системне програмне забезпечення, інженерію програмного забезпечення, комп'ютерні мережі.

Особливості дисципліни, методи та технології навчання

Лекції проводяться з використанням мультимедійних технологій, в тому числі, інтерактивного хмарного середовища Microsoft Teams.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Захист інформації. Системи за засоби захисту
Вступ. Аналіз можливих каналів витоку інформації, що зберігається в КС. Класифікація можливих каналів витоку інформації в КС. Модель порушника
Захист операційної системи. Компоненти забезпечення захисту. Безпека системних даних
Ознаки присутності шкідливих програм. Безпека системних та офісних програми
Реалізація функцій системи розмежування доступу. Аналіз систем захисту від НСД. Системи захисту інформації. Вимоги до систем розподілення доступу. Парольний захист.
Комп'ютерна вірусологія. Принципи функціонування комп'ютерних вірусів. Класифікація комп'ютерних вірусів. Технологія застосування засобів захисту від вірусів
Тема 2. Захист від несанкціонованого використання

Системи захисту від копіювання. Технічні відомості.. Запис і читання секторів диску. Доступні області диску. Захист жорсткого диску. Розмежування доступу до дискового простору диску. Методи відновлення інформації. Методи повного знищення інформації на носіях.
Захист оптичних носіїв інформації. Особливості роботи оптичних приводів. Фізична та інформаційна структура оптичних дисків. Захист CD- и DVD-дисків. Нанесення міток, які не копіюються. Побудова твін-секторів. Визначення та приєднання до унікальності топології диску. Технології захисту: AACS, HDCP, MMC, CSS, RPC, SafeDisc, StarForce.
Засоби захисту, що спираються на системну плату і систему BIOS. Застосування методів захисту орієнтованих на BIOS.
Захист від відлагодних засобів. Архітектура процесору та операційного середовища. Конвеєр команд процесору. Засоби протидії дизасемблюванню програм. Заміна на еквіваленти. Динамічне перетворення коду.

Тема 3. Криптографія.

Вступ. Класифікація криптографічних алгоритмів. Основні криптографічні методи
Симетричні криптографічні системи. Загальні складові. Шифри заміни. Шифри підстановки. Шифри перестановки.
Поточні алгоритми. Шифрування за допомогою датчика псевдовипадкових чисел. Моно- та багатоалфавітні шифри. Би-грами. Сучасні потокові криптоалгоритми
Блочні алгоритми. Схеми використання блочних шифрів. DES - Стандарт США. на шифрування даних. ГОСТ 28147-89 - стандарт на шифрування даних. Сучасні блочні криптоалгоритми.
Системи з відкритим ключем. Алгоритм RSA. Система PGP. Використання та застосування СВК. Цифровий підпис. Хеш-функції. Алгоритм Ель-Гамаля. Алгоритм DSS. Алгоритм SHA. Алгоритм MD2. Алгоритм MD4. Алгоритм MD5.
Криптоаналіз алгоритмов шифрования. Статистичний, лінійний, диференціальний криптоаналіз. Криптоаналіз симетричних систем. Аналіз блокових шифрів. Аналіз систем шифрування на основі датчиків псевдовипадкових шифрів. Аналіз потокових шифрів. Часовий аналіз реалізацій асиметричних систем (Диффи-Хеллмана, RSA, DSS)
Порівняння криптографічних методів. Засоби використання. Недоліки криптоалгоритмів.

Тема 4. Стеганографія.

Стеганографія. Загальні поняття. Стеганографія у текстових файлах. Стеганографія у графічних файлах. Стиснення інформації.

Тема 5. Безпека комп'ютерних мереж.

Захист інформації у мережах. Особливості існуючих засобів атак. Рівні виконання захисту та залежні функції. Протоколи безпеки мереж. Брандмауери та їх застосування. Конфігурації побудови захищених мережених вузлів.

Теми практичних занять

Тема 1. Захист від несанкціонованого доступу в операційній системі.

Захист від несанкціонованого доступу в операційній системі. Керування правами користувачів в операційній системі. Безпека та використання захисту у MS Office

Тема 2. Профілактика шкідливого ПЗ.

Основні ознаки присутності на комп'ютері шкідливих програм. Профілактика проникнення шкідливого програмного забезпечення. Засоби пошуку уразливостей інформаційних систем. Робота антивірусу.

Тема 3. Розробка програми розмежування повноважень користувачів на основі парольної аутентифікації

Тема 4. Захист програмного забезпечення від несанкціонованого використання й копіювання.

Тема 5.Симетрічне шифрування.

Шифрування та дешифрування даних за допомогою блокових алгоритмів (перестановки (збивання), підстановки (заміна). Використання режимів шифрування. Шифрування та дешифрування даних за допомогою потокових алгоритмів. Гамування

Тема 6. Шифрування з відкритими ключами.

Використання алгоритмів шифрування з відкритими ключами. Використання односпрямованих хеш-функцій. Електронно-цифровий підпис

Тема 7. Стеганографічні перетворення.

Стеганографія текстової та графічної інформації.

Тема 8. Безпека мереж.
Засоби пошуку уразливостей мережі. Керування доступом. Протоколи безпеки. Мережна криптографія.

Теми лабораторних робіт

Лабораторні роботи в рамках дисципліни не передбачені

Самостійна робота

Курс передбачає підготовку до виконання практичних занять, результатом є оформлюється звіт у відповідному вигляді.
Курсове проектування проводиться відповідно до методичних матеріалів згідно завдань наданих керівниками.
Студентам також рекомендуються додаткові матеріали (відео, статті, підручники) для самостійного вивчення та аналізу

Література та навчальні матеріали

Основна література:
1. Главчев М.І. Електронний макет конспекту лекційного матеріалу. https://drive.google.com/drive/folders/1Ul1H8NfLvxfZMCPL-f17Ggupu3D1EXrz?usp=sharing
2. Главчев М.І. Електронний практикум з практичних занять. https://drive.google.com/drive/folders/1Ns2dRuf-5Sym3rZAs208JuFA86Ew8Meq?usp=sharing
3. Главчев М.І. Електронний макет до курсового проєктування https://drive.google.com/drive/folders/1adRvfkN1Vh8_d4xTcBXkzHaVFHHMwClL?usp=drive_link
4. Главчев М.І. и др. Захист інформацій в КС та мережах. Захист інсталяцій. Навчальний посібник. Харків. 2007. 230 с.
5. Захист інформації в комп'ютерних системах та мережах : навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251 с

Додаткова література:
6. Богуш В.М. Моніторинг систем інформаційної безпеки: навч. посібник [для студ. вищ. навч. закл.] / В.М. Богуш, А. М. Кудін. К. : ДУІКТ, 2006. 414 с.
7. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
8. Захист інформаційних ресурсів: навчально-методичний посібник до курсу "Захист інформаційних ресурсів" / укл. С. О. Троян. – Умань : [б.в.], 2012.-120 с.
9. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с..

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

100% підсумкової оцінки складаються з результатів оцінювання у вигляді заліку (10%) та поточного оцінювання (90%).
Залік: письмове завдання (2 запитання з теорії) та усна доповідь за необхідності.
Поточне оцінювання: 2 онлайн тести(18%), лабораторні роботи (40%) та практичні заняття (32%).

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