Національний університет
«Острозька академія»

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Кредити та кількість годин: 5 ECTS / 150 годин: лекції - 20 год., лабораторні - 50 год., 2 год. консультації та 78 год. на самостійну роботу, екзамен

I. Опис навчальної дисципліни

Сучасний стан розвитку інформаційних технологій показує стрімкий розвиток методів та засобів захисту інформації в комп'ютерних системах у зв'язку із збільшенням кількості та інтенсивності загроз, що виникають як всередині системи так і за її межами.

Навчальний курс «Технології захисту інформації в комп'ютерних системах» призначений для вивчення організації захисту інформації в комп'ютерних системах, ву якому викладено загальні підходи до розробки моделей загроз та порушників, формування на їх основі заходів захисту інформації. Подано методику створення комплексних систем захисту інформації в автоматизованих та обчислювальних системах. Надано порядок використання нормативних документів в галузі технічного захисту інформації та рекомендації щодо порядку функціонування служб захисту інформації в комп'ютерних системах.

II. Мета та завдання навчальної дисципліни

Мета курсу – набуття теоретичних знань та практичних навичок побудови систем технічного та криптографічного захисту інформації на основі розроблених моделей загроз.

Завданням вивчення дисципліни «Технології захисту інформації в комп'ютерних системах»:

- формування системного підходу до дослідження систем технічного та криптографічного захисту інформації в комп'ютерних системах;
- набуття навиків розроблення моделі загроз та моделі порушника інформаційно-комп'ютерних систем;
- отримання знань порядку застосування існуючих та перспективних технологій захисту інформації.

Перелік програмних компетентностей, що формує навчальна дисципліна:

- загальні:

- ЗК1 - Здатність до абстрактного мислення, аналізу та синтезу;
- ЗК2 - Здатність застосовувати знання у практичних ситуаціях;
- ЗК3 - Знання та розуміння предметної області та розуміння професійної діяльності;
- ЗК9 - Здатність працювати в команді.

- спеціальні:

- СК8 - Здатність проектувати та розробляти програмне забезпечення із застосуванням різних парадигм програмування: узагальненого, об'єктно-орієнтованого, функціонального, логічного,

з відповідними моделями, методами й алгоритмами обчислень, структурами даних і механізмами управління;
- СК12 - Здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення;
- СК13 - Здатність до розробки мережевого програмного забезпечення, що функціонує на основі різних топологій структурованих кабельних систем, використовує комп'ютерні системи і мережі передачі даних та аналізує якість роботи комп'ютерних мереж;
- СК14 - Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

III. Результати навчання

До кінця цього курсу студенти навчаться:
- аналізувати види загроз для інформації в комп'ютерних системах, їх класифікацію та наслідки реалізації; володіти теоретичними основами технічних каналів витоку інформації, способами їх локалізації на об'єктах інформаційної діяльності; застосовувати принципи роботи сучасних симетричних та асиметричних криптоалгоритмів;
- вмітимуть виконувати моніторинг процесів функціонування комп'ютерних мереж та інформаційно-телекомунікаційних систем в умовах реалізації загроз різних класів та впливів зовнішніх дестабілізуючих факторів з метою зменшення їх впливу на процеси обміну даними; застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності; забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних системах з метою реалізації встановленої політики безпеки.

Перелік програмних результатів навчання (ПР), що формує навчальна дисципліна:
- ПР3 - Використовувати знання закономірностей випадкових явищ, їх властивостей та операцій над ними, моделей випадкових процесів та сучасних програмних середовищ для розв'язування задач статистичної обробки даних і побудови прогнозних моделей;
- ПР13 - Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення;
- ПР15 - Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

IV. Програма навчальної дисципліни (структура дисципліни)

№	Тема дисципліни
1	Вступ до курсу. Правовий статус інформації. Поняття інформації з обмеженим доступом.
2	Нормативна база із захисту інформації в Україні. Основні вимоги нормативних документів. Основні положення міжнародного стандарту ISO/IEC15408, ISO/IEC 27002.
3	Вимоги із захисту інформації в багатомашинних багатокористувацьких комплексах. Вимоги до захисту службової інформації від несанкціонованого доступу.

4	Розроблення технічного завдання на створення комплексної системи захисту інформації. Порядок проведення робіт зі створення комплексних систем захисту. Вимоги до комплексної системи захисту інформації та політика безпеки.
5	Розробка проекту комплексної системи захисту інформації. Введення в дію комплексної системи захисту інформації, оцінка захищеності інформації в інформаціно-телекомунікаційних системах.
6	Супровід комплексної системи захисту інформації. Положення про службу захисту інформації в інформаційно-обчислювальних системах. Організація роботи служби захисту інформації.
7	Розроблення та впровадження криптографічних засобів шифрування інформації.
8	Розроблення та комп'ютерна симуляція криптографічних алгоритмів в інформаційно-аналітичних системах
9	Стеганографія. Поняття цифрового підпису. Система генерації, зберігання та обміну ключів.
10	Правові та соціальні аспекти захисту інформації.