Галузь знань: 01 Освіта / Педагогіка
Ступінь вищої освіти: Бакалавр
Спеціальність: 015 Професійна освіта (Комп'ютерні технології)
Освітня програма: Професійна освіта. Комп'ютерні технології
Кафедра інформатики і кібернетики

Навчальна дисципліна
«Захист інформації в комп'ютерних системах»

Семестр – 6

Форма контролю – екзамен

Кількість кредитів ЄКТС – 5

І. Основна мета засвоєння курсу: формування теоретичних знань щодо можливих небезпек і ступеня ризику втрат інформації, а також практичних навичок щодо забезпечення захисту програмної продукції.

ІІ. Місце навчальної дисципліни в освітній програмі

Дисципліна «Захист інформації в комп'ютерних системах» дозволяє набути студентам додаткових професійних компетенцій. Вивчення дисципліни ґрунтується на знаннях, отриманих у курсах «Програмування», «Алгоритми і структури даних», «Операційні системи та системне програмування».

ІІІ. Завдання дисципліни: навчання студентів принципам побудови комплексних систем захисту інформації, розробки, дослідженню та застосуванню механізмів захисту інформації, що засновані на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення автентичності, цілісності та конфіденційності інформаційних систем та технологій (ІС та Т), вивчення студентами основ стеганографічного захисту інформації та особливості побудови інфраструктури відкритих ключів (ІВК).

ІV. Основні знання та уміння, яких набуває студент після опанування даної дисципліни

Основні знання:

– основні положення законодавства в галузі захисту інформації, основні міжнародні та національні стандарти з безпеки ІС та Т;
– основні терміни та визначення політики безпеки, принципи побудови профілю захисту інформації для забезпечення послуг безпеки;
– механізми та протоколи забезпечення конфіденційності ІС та Т;
– механізми та протоколи забезпечення автентичності ІС та Т;
– механізми та протоколи забезпечення цілісності даних ІС та Т;
– модель порушника, основні види атак, принципи криптоаналізу;
– механізми та протоколи керування ключами в ІВК інформаційної системи;
– методи та процедури цифрової стеганографії.

Основні вміння:

– використовувати сучасні криптографічні методи для захисту конфіденційної інформації;
– використовувати систему електронного підпису або режиму електронного цифрового підпису;
– застосовувати систему захисту інформації в автоматизованих системах, включаючи захист конфіденційності;
– передбачати несанкціонований доступ;
– забезпечувати цілісність та конфіденційність даних;
– використовувати біометричні засоби автентифікації та контролю;

– застосовувати методи автентифікації та авторизацію доступу до даних;
– здійснювати ідентифікацію та перевірку користувачів.

V. Короткий зміст дисципліни

Тема 1.Огляд безпеки системи. Основні поняття та визначення безпеки. Роль захисту інформації в ІС, умови функціонування підсистеми безпеки в комп'ютерних мережах та системах. Вимоги щодо безпеки системи, ризики безпеки. Послуги безпеки: конфіденційність, цілісність, автентичність, причетність, спостереженість. Розподіл послуг безпеки за рівнями моделі ISO/OSI. Критерії захищеності комп'ютерних систем. Розробка профілю захисту. Механізми реалізації послуг безпеки. Стандарт ISO-7498-2. Побудування та впровадження систем захисту інформації.

Тема 2. Механізми і політики розмежування прав доступу. Засоби забезпечення захисту інформації в СУБД. Засоби ідентифікації й автентифікації об'єктів баз даних, управління доступом. Засобу контролю цілісності інформації, організація аудиту. Скасування прав доступу. Видача прав доступу до об'єктів баз даних.

Тема 3. Методи та пристрої забезпечення захисту і безпеки. Компоненти криптосистеми та їх функціональні характеристики. Побудова класифікацій криптографічних засобів. Захист інформації за допомогою міжмережних екранів.

Тема 4. Захист, доступ та автентифікація. Загальні механізми забезпечення безпеки. Взаємозв'язок послуг та механізмів безпеки і взаємозв'язок послуг і рівнів моделі взаємодії відкритих систем. Автентифікація даних, механізми забезпечення та методи автентифікації.

Тема 5. Моделі захисту. Захист пам'яті. Побудова моделі порушника безпеки. Організація захисту, захист окремих чарунок пам'яті. Основні засоби захисту пам'яті при керуванні таз привілеями. Моделі безпеки, які застосовуються при побудові захисту в СУБД. Захист БД в системах з видаленим доступом. Інтерфейси CGI, API й FastCGI.

Тема 6. Шифрування даних. Математичні основи сучасної теорії захисту інформації. Методи булевої алгебри, елементи кореляційного та спектрального аналізу. Прості шифри. Симетричне шифрування даних. Криптографічні примітиви й типи структур симетричного шифрування. Блочні симетричні шифри, алгоритми блокового симетричного шифрування DES, ГОСТ-28147,Rijndael. Архітектура блочних симетричних шифрів. Типові режими роботи криптосистеми: "Електронна кодова книга", "Зчеплення блоків шифру", "Зворотний зв'язок з шифру", "Зворотний зв'язок з виходу". Режим простої заміни. Режим гама шифрування. Режим шифрування зі зворотним зв'язком за виходом. Режим вироблення імітовставки. Потокові шифри. Регістри зсуву зі зворотнім зв'язком. Асиметричне шифрування даних. Математичні положення теорії скінченних полів та систем класів лишків. Математичні положення теорії чисел. Асиметричні алгоритми шифрування даних RSA та Ель Гамаля.

Тема 7. Управління відновленням. Захист і відновлення даних. Формування служб резервного копіювання й відновлення даних для критично-важливих серверів. Кластерізація серверів. Етапи управління формуванням плану резервного відновлення. Типи та топології резервного копіювання.

Тема 8. Основні напрями розвитку сучасної криптографії. Основні криптографічні примітиви. Математичні моделі нелінійних вузлів замін у термінах булевої алгебри. Основні напрями розвитку асиметричних криптоалгоритмів. Криптографія на еліптичних кривих. Теоретико-чисельні задачі, складність арифметики точок ЕК в різних формах і представленнях. Цифрова стеганографія з відкритим ключем.

Тема 9. Механізми та протоколи керування ключами в ІВК інформаційної системи. Компоненти та сервіси інфраструктури відкритих ключів. Архітектура і топологія PKI. Стандарти в галузі PKI. Сертифікати відкритих ключів X.509, управління сертифікатами. Системи PKI. Документ політика захисту інформації, його сутність та структура, управління ключами. Профілі безпеки автоматизованих систем. Основні вимоги до політиці PKI.

Тема 10. Основні види атак, принципи криптоаналізу. Основи криптографії. Формальне математичне визначення криптосистеми. Критерії та показники ефективності. Аналіз основних видів атак, рисків та вразливих елементів інформаційних систем. Класифікація криптоаналітичних атак. Диференціальний криптоаналіз, диференціальний криптоаналіз на основі відмов пристрою. Лінійний криптоаналіз. Силова атака на основі розподілених розв'язань.

Тема 11. Алгоритми з секретним ключем. Захист інформації на мережному рівні. Протоколи захисту та цілісності IPSec, SSL, TLS, їх сутність.

Тема 12. Алгоритми з відкритим ключем. Системи захисту PGP та CS MIME. Криптографічні функції. Сумісність на рівні електронної пошти. Захищена електронна пошта.

Тема 13. Протоколи автентифікації. Класифікація механізмів автентифікації. MDC-коди, основні алгоритми. MAC-коди, основні способи формування. Методи побудови універсальних геш-функцій.

Тема 14. Цифрові підписи. Класифікація стандартів електронних цифрових підписів. Моделі цифрових підписів. Основні стандарти цифрового підпису.

Тема 15. Використання паролів і механізмів контролю за доступом. Основні принципи захисту інформації при підключенні до мережі Інтернет. Використання паролів і механізмів контролю.

VI. Назва кафедри та викладацький склад, який буде забезпечувати викладання курсу

Кафедра інформатики і кібернетики факультету інформатики, математики та економіки.

VII. Обсяги навчального навантаження та терміни викладання курсу

На вивчення дисципліни відводиться 150 годин (5 кредитів ЄКТС).

Дисципліна вивчається у 6 семестрі

VIII. Основні інформаційні джерела до вивчення дисципліни

1. Писарчук О.О. Основи захисту інформації : навчальний посібник / О.О. Писарчук, Ю. Г. Даник, С. Г. Вдовенко та ін. – Житомир : ЖВІ ДУТ, 2015. – 226 с.

2. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. – К.: Вид. Національної академії внут. справ, 2012. – 104 с.

3. Кузнецов О.О. Захист інформації в інформаційних системах. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. - Харків: Вид. ХНЕУ, 2011.– 510.

IX. Система оцінювання:

Поточний контроль: оцінювання виконання завдань на лабораторних заняттях, оцінювання 2-х модульних контрольних робіт, виконання індивідуальних проектів.

Підсумковий контроль: екзамен у 6 семестрі.