ЗАХИСТ ІНФОРМАЦІЇ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Семестр	7, 8
Освітньо-професійний ступінь	Фаховий молодший бакалавр
Кількість кредитів ЄКТС	5
Форма контролю	Залік
Аудиторні години	99 (77 год. лекцій, 22 год. лабораторних)

Загальний опис дисципліни

Дисципліна «Захист інформації у комп'ютерних мережах» спрямована на набуття здобувачами фахової передвищої освіти знань і вмінь із розуміння та кваліфікованого застосування в практичній діяльності теоретико-прикладних засад захисту комп'ютерних мереж на різних ієрархічних рівнях.

Мета дисципліни – формування знань і навичок щодо фундаментальних теоретичних положень і практичних аспектів із розробки і впровадження програмно-технічних рішень інформаційних технологій щодо забезпечення безпеки в інформаційних мережах. Під час вивчення даної дисципліни у студентів формуються компетентності щодо вирішення теоретико-прикладних завдань різного призначення і рівня складності, які пов'язані з аналізом, синтезом, проєктуванням і технічним супроводом програмно-технічних рішень щодо забезпечення безпеки в інформаційних мережах.

Завдання курсу:

– опанування теоретико-понятійної бази курсу;

– ознайомлення зі сучасною апаратною і програмною базами побудови систем захисту інформації у комп'ютерних мережах;

– опанування засобів і методів протидії отриманню несанкціонованого доступу до інформаційних ресурсів, захисту адміністративного доступу до мережного обладнання в комп'ютерних мережах на різних ієрархічних рівнях;

– ознайомлення зі сучасними перспективними напрямками концепції захисту комп'ютерних мереж фірми CISCO.

Майбутній фахівець повинен мати наступні компетенції:

Інтегральна компетентність	Здатність вирішувати складні спеціалізовані задачі в галузі інформаційних технологій або у процесі навчання, що вимагає застосування методів і технологій комп'ютерної інженерії та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності; здійснювати контроль інших осіб у визначених ситуаціях.
Загальні компетентності	ЗК6. Здатність спілкуватися іноземною мовою. ЗК8. Здатність вчитися і оволодівати сучасними знаннями.
Спеціальні компетентності	СК3. Здатність вільно користуватись сучасними комп'ютерними та інформаційними технологіями, прикладними та спеціалізованими комп'ютерно-інтегрованими середовищами для розробки, впровадження та обслуговування апаратних та програмних засобів комп'ютерної інженерії. СК6. Здатність брати участь в модернізації апаратних та програмних засобів комп'ютерної інженерії. СК7. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи. СК8. Здатність здійснювати організацію робочих місць з урахуванням вимог охорони праці, їх технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації. СК11. Здатність здійснювати вибір, розгортати, інтегрувати,

	діагностувати, адмініструвати та експлуатувати комп'ютерні системи та мережі, мережеві ресурси, сервіси та інфраструктуру організації. СК13. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їх компонентів шляхом використання аналітичних методів і методів моделювання.

Здобуті знання і вміння відображені в результатах навчання

Результати навчання	РН4. Застосовувати правові норми, норми з охорони праці, безпеки життєдіяльності у професійній діяльності. РН6. Тестувати, діагностувати та обслуговувати апаратні та програмні засоби комп'ютерної інженерії. РН8 Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації апаратних та програмних засобів комп'ютерної інженерії для вирішення технічних задач у професійній діяльності. РН10. Здійснювати пошук інформації з різних джерел для розв'язання задач комп'ютерної інженерії. РН11. Ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів комп'ютерної інженерії. РН12. Поєднувати теорію і практику, знаходити та обґрунтовувати шляхи рішення типових задач у професійній діяльності з урахуванням виробничих інтересів. РН14. Використовувати сучасні інтегровані середовища, методи і технології розробки, впровадження, адміністрування комп'ютерних систем та мереж, баз даних і знань.

Теми лекцій:

1 Вступ. Мета і завдання дисципліни « Захист інформації в комп'ютерних мережах». Основні поняття та визначення. Загальна схема процесу забезпечення безпеки. Загальнодержавна правова база захисту інформації в інформаційних системах. Основні кіберзакони, стандарти та відповідальність. Інтернет-спільноти з кібербезпеки.

2 Кібербезпека – загрози, вразливості та атаки. Типові загрози, атаки та області їх розповсюдження. Характеристика сучасних кібератак на інформаційно-комунікаційні технології. Інструменти і процедури для нейтралізації наслідків впливу шкідливого ПЗ та поширених мережевих атак.

3 Процедури забезпечення безпеки. Фізичний захист. Поточні виправлення й оновлення. Антивірусне ПЗ. Антиспам. Програма захисту від шпигунського і рекламного ПЗ. Засоби блокування спливаючих вікон. Захист даних. Безпека бездротових пристроїв.

4 Криптографічні методи захисту інформації при її передаванні у комп'ютерних мережах. Історичний розвиток криптографії та криптоаналітики. Поняття шифру та коду. Симетричні криптосистеми шифрування. Основні режими роботи та особливості застосування блочного симетричного алгоритму. Алгоритм шифрування DES. Американський стандарт шифрування AES. Схема Фейстеля. Шифр Blowfish.

5 Асиметричні шифри. Розподілення ключів по схемі Діффі-Хеллмана. Криптографічна система RSA. Криптографічна система Эль-Гамаля. Сумісне використання симетричних та асиметричних шифрів.

6 Методи шифрування інформації. Застосування алгоритмів шифрування для забезпечення конфіденційності даних. Шифрування інформації методом з відкритим ключем.

7 Забезпечення безпеки мережевих пристроїв. Захист мережевої інфраструктури. Підходи до захисту граничних маршрутизаторів. Забезпечення захисту адміністративного доступу. Безпечний локальний і віддалений доступ.

8 Технологія захисту AAA. Налаштування засобів AAA сервера мережевого доступу. Архітектура захисту AAA. Призначення AAA. Локальна та групова політики безпеки системи.

Локальна автентифікація AAA. Характеристики та протоколи AAA на основі сервера. Впровадження серверної автентифікації за допомогою протоколів TACACS+ і RADIUS. Серверна авторизація та облік AAA.

9 Впровадження технологій міжмережевого екрану для захисту периметра мережі. Списки контроля доступом. Технології міжмережевих екранів. Зональні міжмережеві екрани (Zone Based Firewal).

10 Впровадження системи запобігання вторгненням (IPS). Методи виявлення вторгнень. Характеристики IDS і IPS. Впровадження IPS. Сігнатури IPS.

11 Впровадження захищених приватних віртуальних мереж (VPN). Призначення і типи мереж VPN. Загальні відомості про IPsec. Компоненти мережі IPsec VPN та їх функціонування. Реалізація мереж Site-to-Site IPsec VPN.

Теми занять:

(семінарських, практичних, лабораторних)

1 Дослідження відомостей про атаки.

2 Дослідження процесу шифрування повідомлення з допомогою таблиці Віженера.

3 Дослідження алгоритму шифрування та системи цифрового підпису Ель Гамаля.

4 Налаштування безпечного адміністративного доступу обладнання Cisco для захисту від злому.

5 Захист адміністративного доступу за допомогою AAA та протоколу RADIUS.

6 Налаштування ACL з метою запобігання атакам.

7 Налаштування системи запобігання вторгнень (IPS).

8 Захист міжмережевих з'єднань Zone-Based Policy Firewall.

9 Налаштування та перевірка Site-to-Site IPsec VPN.