МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Силабус навчальної дисципліни
«Безпека трансакцій у відкритих системах»

Галузь знань	G Інженерія, виробництво та будівництво
Спеціальність	G5 Електроніка, електронні комунікації, приладобудування та будівництво
Освітня програма	Інформаційно-мережна інженерія
Освітній рівень	Другий (магістерський)
Статус дисципліни	Вільного вибору
Мова викладання, навчання та оцінювання	Українська
Курс / семестр	Перший / перший
Кількість кредитів ЄКТС	3
Розподіл за видами занять навчання та годинами навчання	Лекції – 7 (14 годин)
	Лабораторні роботи – 4 (16 годин)
	Практичні заняття – 0 (0 годин)
	Консультації – 3 (6 годин)
	Самостійна робота – 54 годин
Форма підсумкового контролю	Залік
Кафедра	Інформаційно-мережної інженерії
Викладач	Золотарьов Вадим Анатолійович, доцент, к.т.н.

Мета вивчення дисципліни: опанувати сучасні методи захисту інформації в кіберпросторі та інфокомунікаційних системах, вміти визначати кіберінциденти і добирати засоби їхньої нейтралізації.

Результати навчання та компетентності, які формує навчальна дисципліна

Результати навчання	**Компетентності, якими повинен оволодіти здобувач вищої освіти**
ПРН10. Забезпечувати надійність, живучість, завадозахищеність, інформаційну безпеку та пропускну здатність телекомунікаційних та радіотехнічних систем.	**ЗК1.** Здатність до абстрактного мислення, аналізу та синтезу **ЗК6.** Здатність використовувати інформаційні та комунікаційні технології. **ФК4.** Здатність розв'язувати задачі забезпечення надійності, живучості, завадозахищеності, інформаційної безпеки та пропускної здатності телекомунікаційних та радіотехнічних систем з урахуванням економічних, правових, безпекових та інших аспектів

Зміст навчальної дисципліни

Тема № 1. Політика інформаційної безпеки відкритих систем (Поняття трансакції. Відкриті інфокомунікаційні системи. Категорії безпеки. Принципи управління інформаційною безпекою. Відповідальність за ресурси УІБ)

Тема № 2. Кіберінциденти у відкритих системах (Поняття кіберінцидента. Класифікація кіберінцидентів. Класифікація шкідливого програмного забезпечення. Методи захисту відкритих систем від шкідливого програмного забезпечення).

Тема № 3. Класифікація атак на відкриті системи (Атаки, спрямовані на перехоплення даних користувача. Атаки, спрямовані на виявлення даних про ІКМ. Атаки, спрямовані на відмову в обслуговуванні. Атаки Spoofing. Атаки, спрямовані для отримання доступу до операційного середовища. Віддалені атаки типу ін'єкції)

Тема № 4. Ідентифікація та аутентифікація в інфокомунікаційних системах (Ідентифікація, автентифікація та авторизація користувачів у мережі. Багатофакторна авторизація. Взаємна перевірка істинності користувачів. Симетричний протокол Нідгема- Шрьодера. Асиметричний протокол Нідгема- Шрьодера. Протоколи Kerberos, Kerberos-5. Протоколи автентифікації з нульовою передачею знань.

Тема № 5 Контроль доступу (Бізнес-вимоги до контролю доступу. Управління доступом користувача. Дискреційний і мандатний доступ. Рольовий доступ. Відповідальності користувача Контроль доступу до систем та прикладних програм)

Тема № 6 Безпека вебзастосунків (Порушення контролю доступу. Криптографічні збої. Ін'єкційні атаки. Небезпечний дизайн. Невірна конфігурація безпеки. Вразливі та застарілі компоненти. Помилки ідентифікації та автентифікації. Помилки цілісності програмного забезпечення та даних. Ведення журналу безпеки і моніторинг збоїв. Підробка запитів на боці сервера)

Тема № 7 Безпека електронних документів у відкритих системах (Основні критерії безпеки системи електронного документообігу. Резервне копіювання. Безперервне резервне копіювання. Безпека електронної пошти)

Форми та методи оцінювання

Університет використовує 100 бальну накопичувальну систему оцінювання результатів навчання здобувачів вищої освіти.

Поточний контроль здійснюється під час проведення лекційних, лабораторних занять і має на меті перевірку рівня підготовленості здобувача вищої освіти до виконання конкретної роботи і оцінюється сумою набраних балів.

Підсумковий контроль включає семестровий контроль, який проводиться у формі заліку.

Максимально можлива кількість балів за поточний контроль упродовж семестру для дисципліни, форма контролю якої залік – 100 та мінімально можлива кількість балів – 60.

Поточний контроль включає наступні контрольні заходи: захист звітів з лабораторних робіт; самостійна робота за темами.

Детальніша інформація щодо системи оцінювання та накопичування балів з навчальної дисципліни наведена у робочому плані з навчальної дисципліни.