Силабус освітнього компонента
Програма навчальної дисципліни

Виявлення вторгнень

Шифр та назва спеціальності
113 – Прикладна математика

Інститут
ННІ Комп`ютерних наук та інформаційних технологій

Освітня програма
Інтелектуальний аналіз даних

Кафедра
Кібербезпеки

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Вибіркова

Семестр
8

Мова викладання
Українська

Викладачі, розробники

Король Ольга Григорівна
olha.korol@khpi.edu.ua
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 161, з них патентів на корисну модель 18, 11 монографій, з яких 6 колективних монографій, 18 навчальних посібників, 66 статті у закордонних виданнях та фахових виданнях України, у тому числі у наукометричній базі Scopus. Провідний лектор з дисциплін: «Основи соціальної інженерії», «Інформаційна безпека держави», «Менеджмент інформаційної безпеки», «Організація документообігу з обмеженим доступом», «Безпека в соціальних мережах».
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Виявлення вторнень" є вибірковою навчальною дисципліною. Вивчення дисципліни спрямовано на визначення інформації, що потребує захисту на об’єктах критичної інфраструктури (ОКІ). Опанування методів та засобів технічного захисту інформації на ОКІ. Ознайомлення з каналами витоку інформації та підстав їх утворення. Оволодіння навичками роботи із засобами та комплексами виявлення закладних пристроїв несанкціонованого отримання інформації. Оволодіння навичками роботи із засобами та комплексами захисту інформації на ОКІ. Засвоєння порядку проведення обстеження і аналізу ОКІ з метою забезпечення захисту інформації. Оволодіння організаційно-технічними заходами щодо захисту інформації на ОКІ.

Мета та цілі дисципліни

Навчання студентів принципам визначення загальних вимог до кіберзахисту об’єктів критичної інфраструктури, встановлення переліку базових заходів з кіберзахисту, які повинні бути впроваджені на об’єкті критичної інфраструктури, на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації, визначення порядку та критеріїв віднесення об’єктів до об’єктів критичної інфраструктури.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК 1. Здатність учитися й оволодівати сучасними знаннями.
ЗК 2. Здатність застосовувати знання у практичних ситуаціях.
ЗК 4. Здатність бути критичним і самокритичним.
ЗК 6. Здатність до абстрактного мислення, аналізу і синтезу.
ЗК 8. Знання і розуміння предметної області та розуміння професійної діяльності.
СК 3. Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, аналізу, проєктування, керування, прогнозування, прийняття рішень.
СК 5. Здатність розробляти алгоритми та структури даних, програмні засоби та програмну документацію.
СК 7. Здатність розв'язувати професійні задачі за допомогою комп'ютерної техніки, комп'ютерних мереж та Інтернету, в середовищі сучасних операційних систем, із використанням стандартних офісних додатків.
СК 8. Здатність експлуатувати та обслуговувати програмне забезпечення автоматизованих та інформаційних систем різного призначення.
СК 10. Здатність до проведення математичного і комп'ютерного моделювання, аналізу та обробки даних, обчислювального експерименту, розв'язання формалізованих задач за допомогою спеціалізованих програмних засобів.

Результати навчання

РН 2. Володіти основними положеннями та методами математичного, комплексного та функціонального аналізу, лінійної алгебри та теорії чисел, аналітичної геометрії, теорії диференціальних рівнянь, зокрема рівнянь у частинних похідних, теорії ймовірностей, математичної статистики та випадкових процесів, чисельними методами.
РН 24. Вміти застосовувати існуючі та розробляти нові алгоритми і програмні засоби обробки даних вимірювань та спостережень, текстів, сигналів та зображень.
РН 25. Вміти застосовувати сучасні інформаційні технології та програмне забезпечення для обробки великих масивів даних на основі розподілених і хмарних сервісів.

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 20 год., лабораторні роботи – 30 год., самостійна робота – 100 год.

Передумови вивчення дисципліни (пререквізити)

«Математичний аналіз», «Лінійна алгебра», «Аналітична геометрія», «Основи криптології», «Бази даних та інформаційні системи».

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури.
Перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури.
Тема 2. Фізичний захист об'єктів критичної інфраструктури.

Історії битв. Хакери. Вплив загроз. Сучасний центр моніторингу та управління безпекою (SOC). Захист інфраструктурних комунікацій.

Тема 3. Кіберзахист інфраструктури.

Основні кіберзагрози для критичної інфраструктури. Зловмисники та їхні інструменти.

Тема 4. Управління кризовими ситуаціями та ліквідація наслідків.

Як організувати ефективне управління кризовими ситуаціями в критичній інфраструктурі. Реалізація концепції на прикладі ОБС України. Класифікатор загроз. Удосконалена модель інфраструктури АБС. Концептуальна та синергетична моделі безпеки. Удосконалення моделі оцінювання рівня захищеності. Координація дій різних агентів під час кризової ситуації.

Тема 5. Захист телекомунікаційної інфраструктури.

Як можна захистити телекомунікаційні мережі від кібератак. Сегментація і мікросегментація мережі. Моніторинг і централізоване управління. Next Generation Firewall (NGFW). Unified threat management (UTM). Інспекція зашифрованого трафіку. Захист від витоку конфіденційної інформації. Впровадження рішень двофакторної аутентифікації. Об'єднання локальних мереж і віддалений доступ.

Тема 6 Захист електроенергетичної інфраструктури.

Загрози і вразливості для електроенергетичної інфраструктури. Атаки на інфраструктуру Інтернету речей. Стратегії та технології для захисту електроенергетичної інфраструктури. Виклики, які стоять перед міжнародним співробітництвом у сфері захисту енергетичної інфраструктури.

Тема 7. Захист фінансової інфраструктури.

Основні загрози та ризики для фінансової інфраструктури, інструменти для їх виявлення та оцінки. Методи та технології для захисту фінансових транзакцій та даних в банках та фінансових установах. Стандарти та регуляторні вимоги для забезпечення безпеки фінансової інфраструктури. Сучасні тенденції та інновації в галузі кібербезпеки для захисту фінансових систем та інфраструктури.

Тема 8. Міжнародна співпраця у захисті критичної інфраструктури.

Міжнародні організації та ініціативи для координації заходів з захисту критичної інфраструктури між країнами. Міжнародні договори і механізми співробітництва для забезпечення безпеки критичної інфраструктури. Зелена книга з питань захисту критичної інфраструктури в Україні. Сектори, об’єкти, системи, що можуть бути віднесені до критичної інфраструктури. Основні загрози критичній інфраструктурі. Державна політика захисту критичної інфраструктури. Стратегічні цілі державної політики захисту критичної інфраструктури. Основні принципи формування захисту критичної інфраструктури в Україні. Система захисту критичної інфраструктури в Україні. Розвиток механізмів захисту критичної інфраструктури в Україні.

Тема 9. Умови виникнення терористичної загрози та заходи протидії.

Аналіз сутності та змісту проблеми інформаційної безпеки держави на сучасному етапі розвитку науки і техніки. Фактори зародження тероризму. Варіанти класифікації тероризму. Типи терористів. Мотиви терористів. Методи підвищення рівня кіберзахисту критичної інформаційної структури.

Тема 10. Інструментальні засоби управління ризиками інформаційної безпеки об`єктів критичної інфраструктури.

Інструментальні засоби управління ризиками інформаційної безпеки/ Моделі оцінки ризиків компанії Digital Securit. Модель аналізу загроз та вразливостей. Принцип роботи алгоритм. Розрахунок ризиків за загрозою інформаційної безпеки. Завдання контрзаходів. Платіжна інфраструктура.

Тема 11. Система управління як об’єкт кібернетичної безпеки.

Аналіз системи управління як об’єкту кібернетичної безпеки. Особливості аналізу. Основи виявлення та пошуку об’єктів з критичною кібернетичною інфраструктурою.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Вивчення загальних вимог до кіберзахисту об’єктів критичної інфраструктури.

Тема 2. Критична інфраструктура за регіонами України. Організаційні засади регіону України як складові національної системи захисту критичної інфраструктури.
Тема 3. Складання відомостей про об'єкт критичної інформаційної інфраструктури визначеного регіону України.
Тема 4. Вивчення особливостей національної система захисту критичної інфраструктури.
Тема 5. Вивчення особливостей формування Технічних вимог на створення спеціалізованого програмного забезпечення «Державний реєстр об'єктів критичної інформаційної інфраструктури».
Тема 6. Дослідження заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури банків.
Тема 7. Методичні рекомендації щодо розробки поточного та цільового профілю кіберзахисту. Методичні рекомендації щодо аналізу поточного та цільового профілю кіберзахисту.
Тема 8. Проведення класифікації заходів кіберзахисту об'єктів критичної інфраструктури.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт та іспиту.

Література та навчальні матеріали

Основна література

1. Закон України "Про критичну інфраструктуру", від 16.11.2021 № 1882-IX. https://zakon.rada.gov.ua/laws/show/1882-20#Text
2. Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури", від 19 червня 2019 р. № 518. https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
3. Постанова Кабінету Міністрів України "Деякі питання об'єктів критичної інформаційної інфраструктури ", від 9 жовтня 2020 р. № 943. https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text
4. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06 жовтня 2021 року № 601. https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601
5. Закон України "Про критичну інфраструктуру". https://zakon.rada.gov.ua/laws/show/1882-20#Text
6. Постанова Правління Національного банку України "Про затвердження Положення про організацію кіберзахисту в банківській системі України". https://zakon.rada.gov.ua/laws/show/v0178500-22#Text
7. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с. https://profbook.com.ua/index.php?route=product/product/download&product_id=2663&download_id=1094
8. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

Додаткова література

11. ISO/IEC 27001:2022– [Режим доступу: https://www.iso.org/ru/standard/27001
12. ISO/IEC 27002:2022– [Режим доступу: https://www.iso.org/standard/75652.html
13. ISO/IEC 27005:2022– [Режим доступу: https://www.iso.org/standard/80585.html

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 30% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 20% семестрової оцінки;
•іспит: 40% семестрової оцінки

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
28.08.2023 р.

Завідувач кафедри
Сергій ЄВСЕЄВ

Дата погодження, підпис
31.08.2023 р.

Гарант ОП
Олена АХІЄЗЕР