Силабус освітнього компонента
Програма навчальної дисципліни

Безпека інформаційних систем

Шифр та назва спеціальності
126 – Інформаційні системи та технології

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Програмне забезпечення інформаційних систем

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Спеціальна (фахова), Обов'язкова

Семестр
2

Мова викладання
Українська

Викладачі, розробники

Євсеєв Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 337, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 29 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 156 статті у закордонних виданнях та фахових виданнях України, з них 40 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем» , «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Безпека інформаційних систем " є обов`язковою навчальною дисципліною. Навчальний курс призначений для вивчення основних засобів та заходів захисту інформації в інформаційних системах, в якому класифіковано загрози для інформації за критеріями цілісності, конфіденційності та доступності, методів та засобів їх локалізації та блокування. Подано основні принципи формування систем технічного та криптографічного захисту інформації. Надано описи та розглянуто принципи дії сучасних криптоалгоритмів, засобів хешування, генерації та технологій електронного цифрового підпису.

Мета та цілі дисципліни

Отримання здобувачами вищої освіти теоретичних знань та практичних навичок побудови захищених інформаційних систем на основі сучасних засобів технічного та криптографічного захисту інформації, формування системного підходу до побудови захищених інформаційних систем, набуття навиків блокування технічних каналів витоку інформації, отримання знань порядку застосування методів захисту від несанкціонованого доступу.

Формат занять

Лекції, практичні заняття, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК04. Здатність розробляти проекти та управляти ними.
ЗК05. Здатність оцінювати та забезпечувати якість виконуваних робіт.
СК01. Здатність розробляти та застосувати ІСТ, необхідні для розв'язання стратегічних і поточних задач.
СК03. Здатність проектувати інформаційні системи з урахуванням особливостей їх призначення, неповної/недостатньої інформації та суперечливих вимог.
СК06. Здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки.
СК07. Розробляти і реалізовувати інноваційні проекти у сфері ІСТ.

Результати навчання

РН01. Відшуковувати необхідну інформацію в науковій і технічній літературі, базах даних, інших джерелах, аналізувати та оцінювати цю інформацію.
РН04. Управляти процесами розробки, впровадження та експлуатації у сфері ІСТ, які є складними, непередбачуваними і потребують нових стратегічних та командних підходів.
РН08. Розробляти моделі інформаційних процесів та систем різного класу, використовувати методи моделювання, формалізації, алгоритмізації та реалізації моделей з використанням сучасних комп'ютерних засобів.
РН10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 20 год., практичні роботи – 20 год., самостійна робота – 50 год.

Передумови вивчення дисципліни (пререквізити)

Розробка та впровадження інформаційних систем.

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. Правові аспекти безпеки інформаційних систем.
Закон України "Про інформацію". Закон України "Про науково-технічну інформацію". Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". Закон України "Про основні засади забезпечення кібербезпеки України". Закон України "Про державну таємницю". Закон України "Про захист персональних даних". Регламент європейського

Парламенту і Ради. GENERAL DATA PROTECTION REGULATION. Інтеграція управління ризиком у життєвий цикл розвитку систем (SYSTEM DEVELOPMENT LIFE CYCLE, SDLC). Єдині критерії оцінки безпеки інформаційних технологій ISO/IEC 15408. Рамкова програма з кібербезпеки.

Тема 2. Напрямки забезпечення безпеки інформаційних систем.

Канали несанкціонованого отримання даних. Вимикачі електромагнітних коливань. Низькочастотні випромінювачі. Високочастотні випромінювачі. Оптичні вимикачі. Залежність коефіцієнта згасіння від довжини хвилі. Інфрачервоне поглинання. Електричне поле. Магнітне поле. Аналітичне представлення електромагнітної обстановки. Рішення завдання з забезпечення електромагнітної обстановки. Класифікація акустичних каналів витоку інформації. Середовище поширення і спосіб перехвату. Заходові методи. Беззаходові методи. Напрямки забезпечення інформаційної безпеки. Організаційний захист. Заходи безпеки. Служба безпеки. Системи контролю доступу. Правовий і технічний захист інформації. Аналіз ризиків.

Тема 3. Способи захисту інформації.

Забезпечення інформаційної безпеки. Організаційні заходи. Організаційно-технічні заходи. Характеристика захисних дій. Система безпеки. Основні положення політики безпеки. Моделі сектретних систем. Класифікація цифрових підписів. Механізми аутентифікації у стеку TCP/IP. Механізми аутентифікації у стеку PSEC. Схеми проходження IP-пакету даних в транспортному режимі.

Тема 4. Основні моделі інформаційних систем.

Основні моделі інформаційної безпеки. Дискреційне розмеження доступу. Моделі на основі матриці доступу. Моделі поширення прав доступу. Моделі безпеки на основі тематичної політики. Ієрархічна система ролів. Дводольна система робочих груп. Концепція побудування синергетичної моделі загроз безпеки банківських інформаційних ресурсів.

Тема 5. Внутрішні та зовнішні загрози. Використання IDS та IPS.

Ключові критерії для класифікації кіберінцидентів від легких до складних. Вразливості IP. Атаки на основі ICMP. Атаки за методом підсилення та відбиття. Атаки з підміною адрес. Вразливості TCP та UDP. Атаки на те, що ми робимо. Корпоративні сервіси. Класифікатор загроз. Системи виявлення/запобігання вторгнень. Оцінювання сповіщень Security Onion. Способи моніторингу системи. Інструменти аналізу. Генерація сповіщень. Способи моніторингу системи.

Тема 6. Фізичний захист об'єктів інформаційних систем.

Зламування особистих даних. Компанії, які стали жертвою шантажу. Країни, які зазнали нападу. Хакери Непрофесіонали. Хакери Хактивісти. Вплив загроз. Сучасний центр моніторингу та управління безпекою (SOC). Фізичний захист об`єктів критичної інфраструктури. Захист інфраструктурних комунікацій.

Тема 7. Управління кризовими ситуаціями та ліквідація наслідків.

Організація ефективного управління кризовими ситуаціями в критичній інфраструктурі. Класифікатор загроз. Удосконалена модель інфраструктури АБС. Моделі безпеки. Координація дій різних агентів під час кризової ситуації.

Тема 8. Класифікація кіберінцидентів.

Ключові критерії для класифікації кіберінцидентів від легких до складних. Вразливості IP. Атаки на основі ICMP. Атаки за методом підсилення та відбиття. Атаки з підміною адрес. Вразливості TCP та UDP. Атаки на те, що ми робимо. Корпоративні сервіси. Класифікатор загроз.

Тема 9. Деструктивні методи соціальної інженерії.

Сутність соціальної інженерії. Розуміння поведінки людей. Розробка стратегій впливу. Виявлення вразливостей. Підходи ло визначення сутності соціальної інженерії. Захист від деструктивних методів соціальної інженерії. Вторгнення і заходи протидії. Фішинг (цільовий Фішинг). Зворотна соціальна інженерія. Методи маніпуляції людьми.

Тема 10. Інструментальні засоби управління ризиками інформаційної безпеки.

Моделі оцінки ризиків компанії Digital Security. Модель аналізу загроз та вразливостей. Модель аналізу загроз та вразливостей. Завдання контрзаходів. Зниження часу відновлення функціонування. Збереження даних у платіжній інфраструктурі. Виявлення загроз у платіжній інфраструктурі. Управління кіберризиком.

Теми практичних занять

Тема 1. Характеристика стандартів із забезпечення кібербезпеки.

Тема 2. Міжнародний стандарт з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).

Тема 3. Дослідження заходів безпеки інформаційних систем.
Тема 4. Вивчення та аналіз основних моделей інформаційних систем
Тема 5. Аналіз загроз для інформаційних систем . Призначення, наслідки, протидія.
Тема 6. Розгляд заходів від внутрішніх та зовнішніх загроз. Використання IDS та IPS.
Тема 7. Міжнародні правові інструменти і механізми протидії інформаційним порушенням та кіберзлочинності.
Тема 8. Дослідження стійкості захисту інформаційних систем.
Тема 9. Соціальна інженерія. Вивчення мережевих атак, а також інструменти для аудиту безпеки і проведення атак.
Тема 10. Дослідження та аналіз основних моделейзагроз та вразливостей інформаційних систем.

Теми лабораторних робіт

Лабораторні роботи в рамках дисципліни не передбачені.

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 заліку.
Неформальна освіта
Студентам за темами дисципліни пропонується проходження курсів академії CISCO Інституту комп'ютерних наук та інформаційних технологій (керівник академії – завідувач кафедри кібербезпеки, проф. Євсеєв С.П.)

Література та навчальні матеріали

Основна література:

1. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом "Родовід", 2014. – 428 с.
2. М.В. Захарченко, В.Г. Кононович, В.Й. Кільдішев, Д.В. Голев. «Інформаційна безпека інформаційно-комунікаційних систем: навчальний посібник. Лабораторний практикум. Частина 1. Комплекси засобів захисту інформації від НСД.». - 2011.
3. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.
4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
5. 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.
6. 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.

Додаткова література :

1. ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model. URL: https://www.iso.org/search.html?q=15408-1.
2. ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components. URL: https://www.iso.org/search.html?q=15408-2&hPP=10&idx=all_en&p=0.
3. ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components. URL: https://www.iso.org/search.html?q=15408-3&hPP=10&idx=all_en&p=0.
4. Хорошко В. А. Методи та засоби захисту інформації. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с.
5. Безпека інформаційно-коммунікаційних систем. К. : Видавнича група BHV, 2009. – 608 с.

Askoxylakis I., Ioannidis S., Katsikas S.K., Meadows C. (eds.) Computer Security - ESORICS 2016, Part I.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Підсумкова оцінка з дисципліни - залік, розраховується як середня з кількох складових, що враховує оцінки кожного виду контролю.
Поточне оцінювання:
•практичні заняття: 80% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% 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

29.08.2024 Завідувач кафедри кібербезпеки
Сергій ЄВСЕЄВ

29.08.2024 Гарант ОП
Наталія ХАЦЬКО