



Силабус освітнього компонента Програма навчальної дисципліни



Інформаційна безпека

Шифр та назва спеціальності

124 – Системний аналіз

Інститут

ННІ Комп'ютерних наук та інформаційних технологій

Освітня програма

Системний аналіз і управління

Кафедра

Системного аналізу та інформаційно-аналітичних технологій

Рівень освіти

Магістр

Тип дисципліни

Професійна, вибіркова

Семестр

2

Мова викладання

Українська

Викладачі, розробники



Колбасін Вячеслав Олександрович

viacheslav.kolbasin@khpі.edu.ua

Кандидат технічних наук, доцент кафедри системного аналізу та інформаційно-аналітичних технологій НТУ "ХПІ"

Досвід роботи – 20 років. Автор понад 40 наукових та навчально-методичних праць. Провідний лектор з дисциплін: «Програмування та підтримка веб-застосувань», «Платформи корпоративних інформаційних систем», «Обробка великих обсягів даних у корпоративних системах», «Технології обробки великих обсягів даних». Має професійні сертифікації: AWS Certified Solutions Architect – Associate, AWS Certified Machine Learning – Specialty, Oracle Certified Associate Java SE7, Oracle Certified Professional Java SE7

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Дисципліна спрямована на опанування принципів та засобів інформаційної безпеки. Розглянуто криптографічні методи захисту інформації та базові криптографічні протоколи, засоби інформаційної безпеки що є в сучасних операційних системах, безпека в комп'ютерних мережах та веб-середовищі, розробка архітектури захищених систем та моделювання ризиків. В ході лабораторних робіт студентами ознайомлення з технічними засобами інформаційної безпеки.

Мета та цілі дисципліни

Метою викладання дисципліни є формування у студентів теоретичних знань і практичних навичок з інформаційної безпеки як для повсякденного використання, так і при розробці програмного забезпечення та побудові інформаційних систем, у всіх аспектах забезпечення інформаційної безпеки - криптографічних, технічних та організаційних.

Формат занять

Лекції, лабораторні роботи, консультації, курсова робота, самостійна робота. Підсумковий контроль – залік.

Компетентності

СК2. Здатність проектувати архітектуру інформаційних систем.

СК7. Здатність управляти робочими процесами у сфері інформаційних технологій, які є складними, непередбачуваними та потребують нових стратегічних підходів.

Результати навчання

РН1. Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері системного аналізу та інформаційних технологій і є основою для оригінального мислення та проведення досліджень.

РН9. Розробляти та застосовувати моделі, методи та алгоритми прийняття рішень в умовах конфлікту, нечіткої інформації, невизначеності та ризиків.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредитів ECTS): лекції – 32 год., лабораторні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Для успішного вивчення дисципліни необхідно мати знання та практичні навички з дисципліни "Сучасні методи математичного та комп'ютерного моделювання".

Особливості дисципліни, методи та технології навчання

Лекції проводяться з використанням мультимедійних технологій. Для виконання частини лабораторних робіт використовується віртуальна машина, образ якої є в навчальних матеріалах. Навчальні матеріали доступні студентам через OneDrive кафедри.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Вступ.

Задача інформаційної безпеки. Моделі та рівні загроз для інформаційних систем. Технічні та організаційні методи інформаційної безпеки. Задача криптографії.

Тема 2. Основи симетричної криптографії.

Шифри підстановки та перестановки. Блочні шифри. Шифри Файстеля. Режими використання блочних шифрів. Атаки на симетричні шифри та їх стійкість.

Тема 3. Використання методів симетричної криптографії.

Криптографічні хеш-функції. Підтвердження автентичності повідомлення. Проблема розподілу ключів. Алгоритм Діффі-Геллмана розподілу ключів.

Тема 4. Основи асиметричної криптографії.

Ідея криптографії з відкритим та секретним ключами. Алгоритм RSA. Алгоритми на основі еліптичних кривих. Атаки на асиметричні шифри та їх стійкість.

Тема 5. Протоколи асиметричної криптографії.

Передача зашифрованого повідомлення одному отримувачу. Розповсюдження підтвердженого повідомлення багатьом отримувачам. Інфраструктура відкритого ключа та сертифікати.

Тема 6. Сучасні криптографічні протоколи.

Інфраструктура відкритого ключа та сертифікати. Протокол Kerberos.

Тема 7. Автентифікація користувача.

Парольна автентифікація та її реалізація. Біометрична автентифікація. Багатофакторна автентифікація. Головні загрози для всіх видів автентифікації.

Тема 8. Моделі розподілу доступу.

Головні моделі розподілу доступу. Рольова та атрибутивна моделі. Реалізація цих моделей у ОС Windows.

Тема 9. Засоби операційних систем для шифрування та розподілу доступу.

Захист даних у файлах. Налаштування обмежень доступу та шифрування. Відновлення даних. Експорт та імпорт ключів шифрування. Відстеження спроб несанкціонованого доступу.

Тема 10. Безпека даних в комп'ютерних мережах.

Мережеві загрози інформаційних систем. Мережеві екрани (firewalls). Перехоплення трафіку. Аналіз мережевого трафіку в комп'ютерах під управлінням ОС Windows.

Тема 11. Безпека у веб середовищі.

Протокол HTTP та його загрози. Шифроване з'єднання та сертифікати сайтів. Куки та відстеження історії відвідувань сайтів.

Тема 12. Зловмисне програмне забезпечення.

Комп'ютерні віруси. Мережеві черві. Бекдори. Шпигунські програми. Засоби боротьби з зловмисним ПЗ.

Тема 13. Соціальна інженерія та організаційні засоби інформаційної безпеки.

Методи соціальної інженерії. Фішинг. Телефонний фішинг. Засоби протидії шахрайству в ІТ сфері.

Тема 14. Забезпечення інформаційної безпеки ПЗ що розробляється.

Інформаційна безпека при розробці ПЗ. Бази загроз, включення розпізнавання загроз в CI/CD.

Тема 15. Моделі загроз інформаційних систем.

Карти загроз інформаційних систем. Модель STRIDE. Архітектурні принципи розробки ПЗ, що забезпечують інформаційну безпеку

Тема 16. Оцінка безпеки інформаційних систем.

Тестування інформаційної безпеки. Етичне хакерство та тестування на проникнення.

Теми практичних занять

Практичні заняття в рамках дисципліни не передбачені

Теми лабораторних робіт

Тема 1. Реалізація простих криптографічних алгоритмів.

Тема 2. Шифрування/дешифрування файлів за допомогою AES-256.

Тема 3. Використання асиметричної криптографії для шифрування файлів.

Тема 4. Створення власного сертифікату та його використання.

Тема 5. Перевірка стійкості методів автентифікації.

Тема 6. Реалізація захисту файлів та відстеження спроб несанкціонованого доступу у ОС Windows.

Тема 7. Перехоплення веб-трафіку та куків. Налаштування захищеного з'єднання.

Тема 8. Створення моделі загроз веб-магазину.

Самостійна робота

Дисципліна передбачає виконання індивідуальної розрахункової роботи щодо забезпечення безпеки веб-магазину. Результат роботи оформлюється у письмовий звіт.

Студентам рекомендуються додаткові матеріали для самостійного ознайомлення та вивчення.

Література та навчальні матеріали

Основна література

1. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека: навч. посібник. Харків: Вид. ХНЕУ, 2008. 352 с. URL: <http://www.repository.hneu.edu.ua/jspui/handle/123456789/3068>

2. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с. URL:

<http://eztuir.ztu.edu.ua/jspui/bitstream/123456789/8092/1/%D0%A9%D1%83%D1%80.pdf>

3. Гарнавський Ю.А. Технології захисту інформації: підручник. Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с. URL: <https://ela.kpi.ua/items/7d134482-6de9-4ba1-871b-21306b5c02e9>

4. Демчинський В.В., Грайворонський М.В., Кіреєнко О.В. Основи технологій захисту інформації. Завдання до практичних занять. Київ: КПІ ім. Ігоря Сікорського, 2022. 107 с. URL: <http://files.znu.edu.ua/files/Bibliobooks/Inshi72/0053464.pdf>
5. Ковтунець В.В., Нестеренко О.В., Савенков О.І. Безпека систем підтримки прийняття рішень: навч. посібник. Київ: Національна академія управління, 2016. 190 с. URL: <http://e.ieu.edu.ua/handle/123456789/645>
6. Бурячок В.Л., Киричок Р.В., Складанний П.М. Основи інформаційної та кібернетичної безпеки: навч. посібник. Київ: Київський університет імені Бориса Грінченка, 2018. 320 с. URL: <https://elibrary.kubg.edu.ua/id/eprint/27370/>
7. Fisher D. Application Security Program Handbook. A guide for software engineers and team leaders. Manning. 2022. 296 p. URL: <https://www.manning.com/books/application-security-program-handbook>
8. Richer J., Sanso A. OAuth2 in Action. Manning, 2017, 360 p. URL: <https://www.manning.com/books/oauth-2-in-action>

Додаткова література

1. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th edition. Wiley, 2015. 784 p.
2. Остапов С.Е., Валь Л.О. Основи криптографії: навч. посібник. Чернівці: Книги - XXI, 2008. 188 с.
3. Інформаційна безпека: навч. посібник / Ю.Я. Бобало та ін. Львів: Видавництво Львівської політехніки, 2019. 580 с.
4. Anderson R. Security Engineering, 3rd Edition. Wiley, 2020. 1232 p.
5. Dunkerley M., Tumbarello M. Mastering Windows Security and Hardening, 2nd Edition. Packt publishing, 2022. 816 p.
6. Hoffman A. Web Application Security. O'Reilly Media, 2020. 327 p.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Для оцінки роботи студентів протягом семестру підсумкова оцінка розраховується як середньозважена сума оцінок за контрольні заходи (максимальна сума – 200 балів):

- а) виконання контрольної роботи № 1: максимальна оцінка – 35 балів, вага оцінки – 17.5% кредитів дисципліни);
- б) виконання контрольної роботи № 2: максимальна оцінка – 35 балів, вага оцінки – 17.5% кредитів дисципліни);
- в) виконання лабораторних робіт: максимальна оцінка – 80 балів, вага оцінки – 40% кредитів дисципліни);
- г) виконання розрахункової роботи: максимальна оцінка – 50 балів, вага оцінки – 25% кредитів дисципліни).

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

25.08.2024

Завідувач кафедри
Юрій ДОРОФЄЄВ

25.08.2024

Гарант ОП
Валерій СЕВЕРИН