Силабус освітнього компонента
Програма навчальної дисципліни

Основи безпеки програм та даних

Шифр та назва спеціальності
123 – Комп’ютерна інженерія

Інститут
ННІ комп’ютерних наук та інформаційних технологій

Освітня програма
Сучасне програмування, мобільні пристрої та комп’ютерні ігри (інноваційний кампус/ Прикладна комп’ютерна інженерія)

Кафедра
Комп’ютерна інженерія та програмування (326)

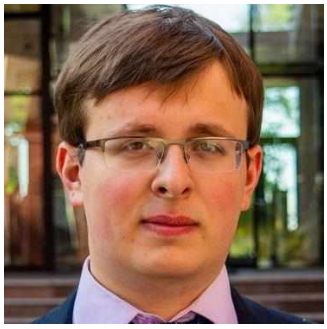
Рівень освіти
Бакалавр

Тип дисципліни
Профільна підготовка

Семестр
6

Мова викладання
Українська

Викладачі, розробники



Челак Віктор Володимирович,
victor@chelak.com.ua;
PhD за спеціальністю 123 Комп'ютерна інженерія, асистент кафедри комп’ютерної інженерії та програмування
Автор та співавтор понад 50 наукових та методичних публікацій.
Основні курси: «Антивірусний захист», «Reverse Programming» (англійською), «Software Means of Information Protection» (англійською), «Основи безпеки програм та даних» та «Штучний інтелект в ігрових програмах».
ORCID: 0000-0001-8810-3394
Посилання на SCOPUS, WoS, Google Scholar:
1. https://www.scopus.com/authid/detail.uri?authorId=57189040595;
2. https://www.webofscience.com/wos/author/record/GZM-2102-2022;
3. https://scholar.google.com/citations?user=lyz9FRQAAAAJ&hl=uk.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Дисципліна розглядає поняття комп'ютерної атаки, принципи побудови систем виявлення вторгнень, провинений рівень аналізу мережевого трафіку та контенту. Значна частина курса присвячена інтелектуальному аналізу даних для систем виявлення та запобігання вторгнень. Теоретичний матеріал підкріплюється додатками з прикладами програмного коду, ілюстраціями та спеціально розробленими прикладами для отримання не лише розуміння, а й навичок використання методів виявлення та стратегій запобігання вторгнень у нетривіальних ситуаціях.

Мета та цілі дисципліни

Формування системи знань з архітектури систем виявлення та запобігання вторгнень, принципів функціонування таких систем та практичні навики розробки систем виявлення та запобігання вторгнень для операційних систем та мережевого захисту.

Формат занять

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

Компетентності

ФК 4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.
ФК 8. Готовність брати участь у роботах з впровадження комп'ютерних систем та мереж, введення їх до експлуатації на об'єктах різного призначення.

Результати навчання

ПРН 1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.
ПРН 8. Вміти системно мислити та застосовувати творчі здібності до формування принципово нових ідей.
ПРН 9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Для вивчення курсу студенти потребують базових знань з дисциплін: «Системне програмування», «Системне програмне забезпечення», «Алгоритми та структури даних» достатніх для:
- знання низькорівневих мов програмування, розробка системних додатків, використовуючи діалекти асемблеру MASM, FASM, TASM або/та NASM;
- створення, завершення процесів ОС, вміння розв'язувати задачі синхронізації;
- знання та розуміння принципів роботи базових алгоритмів на деревах, множинах, структурах даних;
- знання та вміння використовувати алгоритми, що основані на графах;
- знання основних системних функцій WinAPI для роботи з ОС, файловою системою, реєстром, механізмами пасток, тощо.

Крім того курс є базовим для вивчення наступних дисциплін згідно навчального плану: «Програмні засоби захисту інформації», «Прикладна криптологія», «Управління інформаційною безпекою».

Особливості дисципліни, методи та технології навчання

На лекційних заняттях викладання матеріалу здійснюється в усній формі із записом основних положень лекції у конспект. Для демонстрації презентацій застосовується медіа проектор та комп'ютер.

На практичних заняттях здійснюється вивчення принципів функціонування систем виявлення та запобігання вторгнень, які були викладені на лекційних заняттях, та набуття практичних навиків роботи при проектуванні таких систем.
Під час самостійної роботи вдома студенти виконують завдання практичних робот для закріплення матеріалу, який був викладений на лекційних та практичних заняттях.
Додатково, студенти можуть приймати участь в розробці проектів, які передбачені у програмі «Інноваційний кампус» «НТУ» а також неформальної освіти організацій, які забезпечують надання освітніх послуг (NixSolution, GlobalLogic, EPAM та ін.)..

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Комп'ютерні атаки.

Мета та задачі дисципліни. Види комп'ютерних атак. Соціальна інженерія як метод комп'ютерних атак. Фішингові атаки та їх характеристики. Методи інтелектуальних атак.

Тема 2. Принципи побудови систем виявлення вторгнень.

Визначення та роль систем виявлення вторгнень (IDS). Системи виявлення вторгнень на основі сигнатур. Аномалійні системи виявлення вторгнень. Гібридні системи виявлення вторгнень. Методи реагування систем виявлення вторгнень на події.

Тема 3. Технології побудови систем виявлення атак.

Основні принципи систем виявлення атак (IPS). Системи виявлення атак на основі аналізу поведінки. Методи глибокого інспектування для виявлення атак. Системи виявлення атак на основі реал-тайм аналізу. Використання машинного навчання для виявлення атак.

Тема 4. Системи запобігання вторгнень.

Функції та принципи роботи систем запобігання вторгнень (IPS). Захист мережевого периметру за допомогою систем IPS. Використання технологій блокування вторгнень. Проактивні методи виявлення та блокування потенційних атак. Інтеграція систем запобігання вторгнень з іншими засобами безпеки.

Тема 5. Аналіз методів виявлення вторгнень.

Реактивні та проактивні методи виявлення вторгнень. Захист на основі сигнатур та його обмеження. Методи аналізу поведінки для виявлення вторгнень. Застосування машинного навчання в системах виявлення вторгнень. Роль аналізу журналів подій у виявленні вторгнень.

Тема 6. Інтелектуальний аналіз даних в системах виявлення та запобігання вторгнень.

Використання машинного навчання у виявленні атак. Роль штучного інтелекту в адаптивних системах безпеки. Аналіз великих даних для виявлення неочікуваних патернів. Ефективність алгоритмів класифікації в системах безпеки. Використання інтелектуального аналізу даних для прогнозування майбутніх загроз.

Тема 7. Основні компоненти архітектури Firewall.

Архітектура Firewall. Структура Firewall. Ядро Firewall. Структура мережевої ОС. База правил. Модуль управління. Модуль моніторингу та сповіщень. Прикладні посередники.

Тема 8. Модуль самозахисту IPS, IDS.

Техніки захисту від debug інструментів. Техніки захисту від зміни файлів антивірусної системи. Техніки захисту від зміни реєстрових ключів антивірусної системи. Техніки захисту від інструментів Disassembly. Захист від підключення в процес.

Тема 9. Методики оцінки ризиків в IPS та IDS системах.

Поняття ризик. Інформаційний ризик. Загальна серйозність ризику. Факторний аналіз інформаційного ризику (FAIR). Активи, Вразливості, Загрози. Компоненти ландшафту ризику. Декомпозиція ризику по FAIR. Спрощений процес аналізу ризиків (FRAP), переваги та недоліки. Методи обробки ризиків інформаційної безпеки.

Тема 10. Технології безпечного програмування та їх застосування.

Вразливість Buffer Overflow. Stack Protection. Address Space Layout Randomization (ASLR). Data Execution Prevention (DEP). Unbounded execution time DoS. Return-oriented програмування (ROP). Поняття Ботнет. Виявлення елементу Ботнету.

Тема 11. Основні принципи криптографії та їх роль в забезпеченні безпеки програм та даних.

Засоби шифрування та дешифрування інформації. Захист конфіденційності та цілісності даних. Використання хеш-функцій для забезпечення цілісності даних.

Тема 12. Засоби аутентифікації та контроль доступу.

Роль паролів у системах аутентифікації. Двофакторна аутентифікація та біометричні методи. Реалізація механізмів контролю доступу до ресурсів.

Тема 13. Безпека мереж та засоби захисту від мережевих загроз.

Захист від атак типу Man-in-the-Middle. Виявлення та запобігання атакам на мережеві протоколи. Використання віртуальних приватних мереж (VPN) для безпеки мереж.

Тема 14. Стратегії резервного копіювання та відновлення даних.

Планування та виконання резервного копіювання. Синхронізація та забезпечення доступу до резервних копій. Відновлення даних в разі втрати чи пошкодження.

Тема 15. Безпека мобільних додатків та пристроїв.

Аналіз загроз та вразливостей, характерних для мобільних платформ. Використання захисних механізмів у розробці безпечних мобільних додатків. Контроль доступу та безпека даних на мобільних пристроях.

Тема 16. Безпека в хмарних обчисленнях.

Ризики та виклики, пов'язані із використанням хмарних сервісів. Методи шифрування та безпека передачі даних в хмарних системах. Керування доступом та моніторинг безпеки в хмарних обчисленнях.

Теми практичних занять

Практичні занятя в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Реалізація та запобігання комп'ютерним атакам.

Заходи безпеки для захисту від комп'ютерних атак. Принципи конфігурації мережевих систем для зменшення ризиків. Захист від вірусів та шкідливих програм. Захист інформаційних ресурсів корпоративних систем. Створення безпечних паролів та їх управління.

Тема 2. Технології виявлення аномальної активності.

Визначення аномальної активності в мережі. Методи математичного моделювання аномалій. Використання штучного інтелекту для виявлення аномалій. Техніки статистичного аналізу для виявлення аномальностей. Системи кореляції подій для виявлення аномальної активності.

Тема 3. Огляд та особливості сучасних систем виявлення атак.

Тенденції розвитку систем виявлення атак. Використання блокчейн технологій в системах безпеки. Аналіз впровадження інтернету речей у контексті безпеки. Вплив квантового обчислення на системи виявлення атак.

Тема 4. Аналіз мережевого трафіку.

Значення аналізу мережевого трафіку для безпеки. Методи збору та моніторингу мережевого трафіку. Використання пакетних фільтрів для аналізу трафіку. Принципи аналізу SSL/TLS зашифрованого трафіку. Системи інспекції глибокого пакету в аналізі мережевого трафіку.

Тема 5. Методи запобігання вторгнень.

Сегментація мережі як метод запобігання вторгнень. Захист від DDoS-атак та методи їх запобігання. Використання файерволів для блокування небажаних підключень. Принципи роботи систем обнаружения та блокировки вразливостей. Захист від фізичного доступу та соціально-інженерних атак.

Тема 6. Методи пошуку вторгнень.

Аналіз лог-файлів та їх роль у пошуку вторгнень. Використання сигнатур для виявлення атак. Техніки розпізнавання підозрілої активності. Використання тестування на проникнення для пошуку слабких місць. Принципи реал-тайм моніторингу для пошуку нових загроз.

Тема 7. PE-структура. Програми дослідження Malware. xdbg. CFF Explorer. PEiD.

Portable Executable. DOS Header. DOS STUB. COFF Header. Windows Specific Fields. Data Directories. Section Headers Chacteristics. Користування xdbg. Користування CFF Explorer. PEiD та його вразливості.

Тема 8. Аналіз ПЗ комп'ютерної системи.

Типовий вигляд атаки ШПЗ. Аналіз ПЗ комп'ютерної системи. Аналізатор коду. Алгоритм роботи аналізатору коду. Ініціалізація аналізатора коду. Евристичний аналіз. Пошук вірусних сигнатур. Пошук процедури підрахунку дельта. Процедура підрахунку дельта. Повна імітація виконання інструкцій. Зміна параметрів роботи емулятора.

Тема 9. Модуль захисту комп'ютерних систем. Емулятори коду.

Необхідність евристичних підходів та емуляторів. Технологія емулятора коду. Алгоритм роботи. Параметри емулятору. Ініціалізація емулятора. Імітація виконання інструкцій.

Тема 10. Розробка системи моніторингу подій та методів боротьби з ШПЗ.

Моніторинг подій комп'ютерної системи (КС). Механізми пасток (Hook). Карантин програмного забезпечення. Алгоритм компонента карантину в антивірусах. Відновлення файлів після шкоди від ШПЗ. Алгоритм модулю відновлення. Знищення шкідливого ПЗ. Алгоритм знищення шкідливого ПЗ. Запобігання комп'ютерним загрозам.

Тема 11. Розробка сигнатурного аналізатору.

Створення унікальних сигнатур для ідентифікації конкретних видів атак. Аналіз характеристик зловмисного коду та методів атаки. Створення патернів для виявлення аномалій у мережевому трафіку та системних журналах.

Тема 12. Розробка евристичного аналізатору.

Розробка алгоритмів для виявлення нових та невідомих загроз. Засновані на евристичних методах алгоритми для виявлення аномальної активності. Аналіз нестандартних патернів та незвичайних змін у системі.

Тема 13. Побудова штучної нейронної мережі для рішення задачі класифікації стану комп'ютерної системи.

Використання алгоритмів глибокого навчання для автоматичного визначення змін у системі. Аналіз та розпізнавання складних патернів з використанням нейронних мереж. Ідентифікація потенційних загроз за допомогою штучних нейронних мереж.

Тема 14. Штучні імунні мережі та алгоритм DBSCAN.

Використання штучних імунних мереж для відтворення імунних механізмів у системах виявлення вторгнень. Застосування алгоритму DBSCAN для ефективного групування аномальних подій. Визначення кластерів подій у мережевому трафіку чи системних журналах.

Тема 15. Розробка ансамблевих моделей ідентифікації стану комп'ютерних систем та мереж.

Створення ансамблевих моделей, об'єднуючи різні методи виявлення загроз. Використання ансамблю для поліпшення точності ідентифікації стану системи. Аналіз та оцінка ефективності ансамблевих моделей в ідентифікації аномалій.

Тема 16. Методи оцінки якості ідентифікації стану комп'ютерних систем та мереж.

Визначення ключових параметрів для оцінки якості ідентифікації стану системи. Розробка метрик та показників для вимірювання точності та ефективності ідентифікації. Використання стандартів та бенчмарків для порівняння різних систем ідентифікації. Аналіз впливу різних факторів на результати оцінки якості ідентифікації. Розробка стратегій та підходів для постійного покращення процесів ідентифікації в системах безпеки.

Самостійна робота

Опрацьовування лекційного матеріалу.
Підготовка до практичних занять та модульних контролів.
Поглиблене вивчення тем обов'язкового та додаткового характеру, що не розглядались на лекційних заняттях - зазначаються наприкінці кожної лекції окремо.

Література та навчальні матеріали

ОСНОВНА ЛІТЕРАТУРА

1 Axelsson, S. (2000). «Intrusion Detection Systems: A Survey and Taxonomy»
2 Vacca, John R. (2013-08-26). Network and System Security. Elsevier. ISBN 9780124166950.
3 Vacca, John R. (2009-05-04). Computer and Information Security Handbook. Morgan Kaufmann. ISBN 9780080921945.
4 Tripathy, B. and Acharjya, D., 2014. Advances in secure computing, internet services, and applications. Hershey, PA: Information Science Reference.
5 Farooq Anjum; Petros Mouchtaris, "Intrusion Detection Systems," in Security for Wireless Ad Hoc Networks , Wiley, 2007, pp.120-159, doi: 10.1002/9780470118474.ch5.

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

Сайт кафедри комп'ютерної інженерії та програмування: https://web.kpi.kharkov.ua/cep/.
Персональний сайт лектора: https://victor.chelak.com.ua/.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:
модульні контролі - 30 балів; практичні заняття - 40 балів; екзамен - 30 балів.

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 22.04.2024	Завідувач кафедри Олександр ЗАКОВОРОТНИЙ
	Дата погодження, підпис 22.04.2024	Гарант ОП Олександр ЗАКОВОРОТНИЙ