

Силабус курсу

Методологія аудиту захищеності інформаційно-комунікаційних систем

Освітній ступінь – магістр

Галузь знань: 01 Освіта/Педагогіка

Спеціальність: 015.39 Професійна освіта (Цифрові технології)

Освітньо-наукова програма «Професійна освіта (Комп'ютерні технології)»

Кількість кредитів – 5

Рік підготовки, семестр – 2 рік, 4 семестр

Компонент освітньої програми: вибірковий, професійна підготовка

Дні занять: за розкладом, ауд. 233

Консультації: за розкладом, ауд. 205

Мова викладання: українська



Керівник курсу

канд. пед. наук, доцент **Сіткар Тарас Вікторович**

Контактна інформація sitkar@tnpu.edu.ua; 0969415876

Опис дисципліни

Мета дисципліни “Методологія аудиту захищеності інформаційно-комунікаційних систем” полягає в ознайомленні студентів із основами аналізу комп'ютерних систем на проникнення.

У даній дисципліні розглядаються загальні відомості про методи аудиту (аналізу) захищеності комп'ютерних систем від проникнення, зокрема, розглядаються методи збору інформації про комп'ютерну систему, методи сканування, переповнення буфера, DoS атаки, SQL ін'єкції, атаки на веб-сервери, тощо.

На даний час – в епоху активного використання комп'ютерної техніки і широко розповсюдження мережі Інтернет дуже актуальною є проблема захисту інформації, захисту комп'ютерних систем від проникнення. Зокрема, актуальною є проблема аналізу (аудиту) комп'ютерних систем на можливість проникнення і порушення конфіденційності чи доступності інформації.

В результаті вивчення курсу студент повинен знати:

- етапи здійснення аудиту;
- методи та засоби збору інформації про комп'ютерну систему;
- методи та засоби сканування мережі;
- методи та засоби аудиту SQL-ін'єкцій, DoS-атак, перехоплення сесій зв'язку;
- методи та засоби аудиту безпеки операційних систем, веб-серверів та безпроводних систем зв'язку;

В результаті вивчення курсу студент повинен вміти:

- планувати процес аудиту захищеності комп'ютерних систем;

- здійснювати збір інформації про систему;
- проводити сканування мережі;
- здійснювати аналіз системи на можливість проведення SQL-ін'єкцій, DoS-атак, перехоплення сесій зв'язку;
- здійснювати аудит безпеки операційних систем, веб-серверів та безпроводних систем зв'язку.

Курс передбачає лекційні, практичні та лабораторні аудиторні заняття, а також самостійну роботу студента за межами навчального закладу.

Загальний обсяг дисципліни – 150 годин (5 кредити ЄКТС)

З них: 18 год лекції, 32 год практичні та семінарські заняття, 100 год самостійна робота.

Дана дисципліна є вибірковою для вивчення.

Структура курсу

Години (лек. / практ.)	Тема	Результати навчання	Завдання
Змістовий модуль 1 Поняття аудиту, збір інформації, сканування мережі			
1/0	Тема 1 Передумови та поняття аудиту захищеності комп'ютерних систем	У лекції розглядаються передумови аудиту захищеності комп'ютерних систем, етапи його проведення та термінологія.	Питання, кейси, ІНДЗ
1/2	Тема 2 Збір інформації про систему	У лекції розглядається послідовність, методологія та засоби збору інформації про систему.	Питання, кейси, ІНДЗ
	Тема 3 Сканування мережі	У лекції розглядаються типи та методологія сканування, техніки сканування відкритих портів, засоби сканування, техніки підготовки проксі, тунелювання, тощо.	Питання, кейси, ІНДЗ
	Тема 4 Перерахування мережі	У лекції розглядаються концепції і техніки перерахування, засоби перерахування NetBIOS, SNMP, UNIX, LDAP, тощо.	Питання, кейси, ІНДЗ
Змістовий модуль 2 Аудит операційної системи, компютерні Трояни, віруси і червяки, sniffers і соціальна інженерія, DoS та перехоплення сеансу			
2/4	Тема 5 Аудит операційної системи	У лекції розглядається методологія аудиту операційної системи, взлом паролів, підвищення привілеїв, виконання програм, приховування файлів і слідів аналізу.	Питання, кейси, ІНДЗ
2/2	Тема 6 Комп'ютерні трояни і backdoors	У лекції розглядається поняття трояна, принципи його роботи, їх пити, методи виявлення і протидії.	Питання, кейси, ІНДЗ

	Тема 7 Комп'ютерні віруси черв'яки	У лекції розглядаються концепції вірусів і троянів, типи вірусів, їх аналіз і засоби протидії.	Питання, кейси, ІНДЗ
	Тема 8 Sniffers	У лекції розглядаються концепції аналізу трафіку, його типи, приклади аналізу різноманітних протоколів.	Питання, кейси, ІНДЗ
	Тема 9 Соціальна інженерія	У лекції розглядаються концепції соціальної інженерії, її техніки, викрадення персональних даних, методи аудиту захищеності системи на протидію соціальній інженерії.	Питання, кейси, ІНДЗ

Формування програмних компетентностей

Індекс в матриці ОП	Програмні компетентності
ЗК 10	Здатність до розробки й застосування програмного забезпечення виробничого або освітнього процесів.
ФК6	Здатність до розробки, інспекції, інтеграції програмного коду та тестування характеристик програмного забезпечення згідно стандарту ISO 9126.
ФК7.	Здатність до проектування та імплементації компонентних моделей програмного забезпечення як основи крос-платформності.
ФК8.	Здатність працювати з інформацією: знаходити, оцінювати та використовувати інформаційні джерела, здійснювати добір алгоритмів підготовки даних до їх візуалізації згідно методології інфодизайну для інтерпретації результатів наукових і педагогічних досліджень.
ФК11	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в процесі реалізації технологічних процесів у певній галузі професійної діяльності згідно спеціалізації, що передбачає застосування сучасних досягнень науки і техніки та характеризується комплексністю та невизначеністю умов.
ПРН10	Вміти розробляти вимоги та специфікації компонентів інформаційних систем; проектувати та імплементувати компоненти програмного забезпечення; проектувати людино-машинний інтерфейс інформаційних систем; інтегрувати компоненти в систему; розробляти програмні компоненти на стороні сервера.
ПРН24	Аналізувати процес розробки програмного забезпечення з метою оцінки якості; здійснювати ефективні і кваліфіковані інспекції; використовувати статистичні методи для оцінювання щільності дефектів та імовірності відмови.

Літературні джерела

1. Walker M. CEN Certified Ethical Hacker: Exam Guide (All-in-One) / M. Walker – McGraw-Hill Osborne Media; Har/Cdr edition, 2011. – 395 с.
2. Лапони́на О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия / О.Р. Лапони́на. Интернет-университет информационных технологий – ИНТУИТ.ру, 2005. – 608 с.
3. Галатенко В.А. Стандарты информационной безопасности / В.А. Галатенко. Интернет-университет информационных технологий – ИНТУИТ.ру, 2005. – 264 с.
4. Столингс В. Криптография и защита сетей. Принципы и практика, 2-е изд. : Пер. с англ. / В. Столингс. – М.: Издательский дом "Вильямс", 2001. – 672 с.
5. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C (Second Edition) / B. Schneier. – N.Y.: John Wiley & Sons, Inc., 1996. – 758 p.
6. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.
7. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. – СПб: Издательство «Питер», 2000. – 672 с.
8. Олифер В.Г. Сетевые операционные системы / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2001. – 544 с.
9. Кастер Х. Основы Windows® NT и NTFS / Х. Кастер. – М.: Издательский отдел «Русская Редакция» ТОО «Channel Trading Ltd.», 1996. – 440 с.
10. Seth T.R. UNIX System Security Tools / T.R. Seth. – N.Y.: McGraw-Hill, 2000. – 444 p.
11. Неме́т Э. UNIX: руководство системного администратора / Э. Неме́т, Г. Снайдер, С. Сибасс, Т.Р. Хейн. – К.: BHV, 1998 – 832 с.
12. Касперски К. Техника сетевых атак / К. Касперски. – М.: «СОЛОН-Р», 2001. – 396с.
13. Касперски К. Техника и философия хакерских атак / К. Касперски. – М.: «СОЛОН-Р», 2001. – 272 с.
14. Касперски К. Фундаментальные основы хакерства / К. Касперски. – М.: «СОЛОН-Р», 2005. – 448 с.
15. Соломон Д. Внутреннее устройство Microsoft Windows 2000 / Д. Соломон, М. Руссинович. – М.: Русская Редакция, 2001. – 752 с.
16. Медведовский И.Д. Леонов Д. Г. Атака на Internet. – 2-е изд. / И.Д. Медведовский, П.В. Семейнов. – М.: ДМК, 1999. – 336 с.
17. Девянин П.Н. Теоретические основы компьютерной безопасности / П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. – М.: Радио и связь, 2000. – 192с.
18. Лукацкий А. Обнаружение атак / А. Лукацкий. – СПб.: БХВ-Петербург, 2001. – 624с.
19. Ховард М. Защищенный код / М. Ховард, Д. Лебланк. – М.: Издательско-торговый дом «Русская редакция», 2003. – 704 с.
20. Тимошенко А.О. Методи аналізу та проектування систем захисту інформації: Курс лекцій / А.О. Тимошенко. – К: Політехніка, 2007. – 174 с.
21. Анин Б. Защита компьютерной информации / Б. Анин. – СПб.: БХВ-Петербург, 2000. – 384 с.
22. Белкин П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных / П.Ю. Белкин, О.О. Михальский, А. С. Першаков и др. – М.: Радио и связь, 2000. – 168 с.
23. Богуш В.М. Інформаційна безпека від А до Я / В.М. Богуш, А.М. Кудін. – К.: МОУ, 1999. – 456 с.
24. Алферов А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемуш-кин. – М.: Гелиос АРВ, 2001. – 480 с.
25. Бабаш А.В. Криптография / А.В. Бабаш, Г.П. Шанкин – М.: СОЛОН-Р, 2002. – 512с.
26. Конеев И.Р. Информационная безопасность предприятия / И.Р. Конеев, А.В. Беляев. – СПб.: БХВ-Петербург, 2003. – 752 с.
27. Саломая А. Криптография с открытым ключом / А. Саломая. – М.: Мир, 1995. – 318с.
28. Чмора А.Л. Современная прикладная криптография / А.Л. Чмора. – М.: Гелиос АРВ, 2001. – 256 с.
29. Грушо А.А. Теоретические основы защиты информации / А.А. Грушо, Е.Е. Тимонина. – М.: Издательство Агентства «Яхтсмен», 1996. – 187 с.
30. Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников. – М.: Финансы и статистика; Электронформ, 1997. – 368 с.

31. Проскурин В.Г. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах / В.Г. Проскурин, С.В. Крутое, И.В. Мацкевич. – М.: Радио и связь, 2000. – 168 с.
32. Шеховцов В.А. Оперативные системы / В.А. Шеховцов. – К: Видавнична група BHV, 2005. – 576 с.

Політика оцінювання

- **Політика щодо дедлайнів та перескладання:** Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності балів). Перескладання модулів відбувається із дозволу навчальної частини за наявності поважних причин (наприклад, лікарняний).
- **Політика щодо академічної доброчесності:** Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття.
- **Політика щодо відвідування:** Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

Остаточна оцінка за курс розраховується наступним чином:

Види оцінювання		% від остаточної оцінки
Модуль 1	усне опитування, тести, завдання	30
Модуль 2	усне опитування, тести, завдання	30
ІНДЗ		10
Підсумковий контроль – тести		30

Шкала оцінювання студентів:

ECTS	Бали	Зміст
A	90-100	відмінно
B	85-89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом