МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТАВРІЙСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В.І. ВЕРНАДСЬКОГО
Навчально-науковий інститут муніципального управління
та міського господарства
Кафедра загальноінженерних дисциплін та теплоенергетики

ЗАТВЕРДЖУЮ
Директор навчально-наукового
інституту муніципального управління
та міського господарства
_____В.Б. Кисельов
3 вересня 2019 р.

НАВЧАЛЬНА РОБОЧА ПРОГРАМА

дисципліни «Захист інформації в комп'ютерних системах»
(повна назва навчальної дисципліни)
для студентів заочної форми навчання

галузі знань 12 – "Інформаційні технології"
(шифр і назва галузі)

спеціальність 123 – "Комп'ютерна інженерія"
(шифр і назва спеціальності)

освітня програма "Комп'ютерна інженерія"
(назва освітньої програми)

Київ – 2019

Навчальна робоча програма дисципліни «Захист інформації в комп'ютерних системах» для студентів заочної форми навчання *спеціальності* 123– «Комп'ютерна інженерія» за освітньою програмою «Комп'ютерна інженерія»- 9 с.

Розробники: старший викладач Юсипів Т. В.

Робочу програму схвалено на засіданні кафедри загальноінженерних дисциплін та теплоенергетики

Протокол № 1 від 28 серпня 2019 року

Завідувач кафедри
Загальноінженерних дисциплін
та теплоенергетики _____ Медведєв М.Г.

ВСТУП

Навчальна дисципліна «Захист інформації в комп'ютерних системах» є складовою освітньо-професійної програми підготовки фахівців за освітньо-кваліфікаційним рівнем «бакалавр» галузі знань 12 – «Інформаційні технології» *зі спеціальності 123* – «Комп'ютерна інженерія» за освітньою програмою « Комп'ютерна інженерія».

Дана дисципліна є нормативною.

Викладається в 1-му семестрі для 4-го курсу заочної форми навчання в **обсязі – 20 год.**, зокрема: *лекції – 10 год., практичні – 10 год*. Завершується дисципліна – **заліком.**

Мета дисципліни – оволодіння студентами практичними аспектами роботи комп'ютерних систем та засобами їх безпечної роботи, захисту від «злому» інформації і т.ін.

Завдання – дати всебічний огляд що являє собою сучасна комп'ютерна система, які в неї засоби захисту, які сучасні методи та технології застосовуються для захисту інформації в комп'ютерних системах.

У курсі розглядаються також деякі необхідні математичні розділи, як теорії шифрування, основи теорії чисел, елементи теорії множин та комбінаторики.

Курс складається з 1 змістового модуля та 3 тем.

У результаті вивчення навчальної дисципліни студент повинен

знати: базові поняття з дисципліни та методи захисту інформації;

вміти: демонструвати практичні навички для виявлення слабких місць комп'ютерних систем та визначення методів задля запобігання «злому» інформації чи інших методів її захисту.

Місце дисципліни *(у структурно-логічній схемі підготовки фахівців за відповідною освітньою програмою)*. Нормативна навчальна дисципліна «Захист інформації в комп'ютерних системах» є складовою циклу професійної та практичної підготовки фахівців освітньо-кваліфікаційного рівня „бакалавр" за спеціальністю 123 – «Комп'ютерна інженерія» за освітньою програмою «Комп'ютерна інженерія».

Зв'язок з іншими дисциплінами. Серед довгого переліку пов'язаних з курсом дисциплін можна виділити наступні: алгебра і теорія чисел, комбінаторика, теорія ймовірностей, математична логіка та теорія алгоритмів, програмування, методи оптимізації. Враховуючи фундаментальність математичних понять, які розглядаються в цьому курсі дана дисципліна ведеться на 4-му курсі, коли вже в достатній мірі освоєні інші необхідні дисципліни та легко виявляються міждисциплінарні зв'язки між ними.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕМА 1. Основи забезпечення інформаційної безпеки (*4 год.*)

Концептуальні питання створення, функціонування, розвитку і використання національної системи конфіденційного зв'язку. Історія розробки стандартів захисту інформації. Основні положення базового міжнародного стандарту ISO/IEC 15408 "Common Criteria". Основні відомості та структура загальних критеріїв. Процес розробки та кваліфікаційного аналізу. Таксономія вимог, функціональні вимоги, вимоги гарантій. Послуги і механізми захисту інформації.

ТЕМА 2. Основні загрози інформаційної безпеки комп'ютерних систем та мереж (*8 год.*)

Порушення комп'ютерних систем, методи протидії порушенням. Методика вторгнення порушника та методи протидії їй. Стратегії вибору пароля. Розподілені системи виявлення порушень. Програмні зазори, віруси, антивіруси. Антивірусний захист. Спам та методи боротьби зі шкідливим спамом.

ТЕМА 3. Системи захисту інформації в глобальній комп'ютерній мережі (*8 год.*)

Безпека інформації в мережі Інтернет. Найбільш поширені сервіси, що залежать від роботи глобальної мережі. Захист електронної пошти, система PGP. Криптографічні ключі та зв'язки ключів. Система S/MIME. Формат поштового повідомлення (RFC-822). Захист інформації в електронних платіжних системах. Електронні пластикові картки та засоби їх захисту. Управління доступом в мережевій технології «клієнт-сервер» для базових операційних систем.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ І ПРАКТИЧНИХ ЗАНЯТЬ

№ п/п	Назва лекції	Кількість годин		
		лекції	практичні	С/Р
1	**Тема 1.** *Основи забезпечення інформаційної безпеки*	2	2	
2	**Тема 2.** *Основні загрози інформаційної безпеки комп'ютерних систем та мереж*	4	4	
3	**Тема 3.** *Системи захисту інформації в глобальній комп'ютерній мережі*	4	4	
	УСЬОГО	**10**	**10**	**0**

Загальний обсяг **22** *год.,* у тому числі:

лекції **– 10** *год*.

практичні **– 10** *год*.

залік (+консультація до заліку) – **2** *год*.

ТЕМА 1. Основи забезпечення інформаційної безпеки (*4 год.*)

Концептуальні питання створення, функціонування, розвитку і використання національної системи конфіденційного зв'язку. Історія розробки стандартів захисту інформації. Основні положення базового міжнародного стандарту ISO/IEC 15408 "Common Criteria". Основні відомості та структура загальних критеріїв. Процес розробки та кваліфікаційного аналізу. Таксономія вимог, функціональні вимоги, вимоги гарантій. Послуги і механізми захисту інформації.

Практичне заняття 1*. – 2 год*.

ТЕМА 2. Основні загрози інформаційної безпеки комп'ютерних систем та мереж (*8 год.*)

Порушення комп'ютерних систем, методи протидії порушенням. Методика вторгнення порушника та методи протидії їй. Стратегії вибору пароля. Розподілені системи виявлення порушень. Програмні зазори, віруси, антивіруси. Антивірусний захист. Спам та методи боротьби зі шкідливим спамом.

Практичні заняття 2,3*. – 4 год.*

ТЕМА 3. Системи захисту інформації в глобальній комп'ютерній мережі (*8 год.*)

Безпека інформації в мережі Інтернет. Найбільш поширені сервіси, що залежать від роботи глобальної мережі. Захист електронної пошти, система PGP. Криптографічні ключі та зв'язки ключів. Система S/MIME. Формат поштового повідомлення (RFC-822). Захист інформації в електронних платіжних системах. Електронні пластикові картки та засоби їх захисту. Управління доступом в мережевій технології «клієнт-сервер» для базових операційних систем.

Практичні заняття 4,5*. – 4 год.*

Контрольні запитання та завдання

1. Дайте визначення термінам: інформація, інформація з обмеженим доступом, секретна інформація, конфіденційна інформація, захист інформації.

2. Дайте визначення національній системі конфіденційного зв'язку.

3. З якою метою було розроблено еталонну модель OSI?

4. Скільки класів функцій було виділено в моделі OSI? Перерахуйте класи.

5. Дайте класифікацію можливих атак на кожний з рівнів моделі OSI.

6. Перерахуйте базові загальноприйняті послуги безпеки Стандартів ISO 7498, ISO/IEC 10181.

7. Назвіть спеціальні механізми забезпечення безпеки зв’язку

8. В чому суть механізму нотаризації?

9. Що таке цифровий підпис?

10. В чому суть механізму управління маршрутизацією?

11. Дайте визначення автентифікації.

12. Що розуміють під конфіденційністю?

13. Що забезпечує та гарантує послуга управління доступом?

14. Наведіть приклади основних послуг безпеки.

15. Наведіть приклади основних систем і протоколів захисту інформації на прикладному, сеансовому і мережевому рівнях моделі ВВС.

16. Дайте класифікацію порушників.

17. Перерахуйте методи отримання паролів.

18. Які методи протидії порушникам існують?

19. Проілюструйте схему використання паролів у системі UNIX.

20. Які стратегії вибору паролів?

21. Перерахуйте причини необхідності виявлення порушників.

22. Проілюструйте профілі поведінки порушників.

23. Які підходи до розв’язання проблеми виявлення порушників?

24. Проілюструйте розподілену систему виявлення порушень.

25. Опишіть алгоритм створення повідомлення системою PGP.

26. Опишіть алгоритм отримання повідомлення системою PGP.

27. Проілюструйте загальний формат повідомлення PGP.

28. Опишіть алгоритм визначення ступеня довіри ключам.

29. Укажіть причини, за якими алгоритми DES, “потрійний” DES з двома ключами RC2 і RC5 підходить або не підходить для PGP.

30. Опишіть загальні процедури підготовки повідомлень S/MIME. Які криптографічні алгоритми використовуються в S/MIME?

31. Дайте короткий опис типів, підтипів і вмісту S/MIME.

32. Яким чином користувачі оформляють і відновлюють сертифікати S/MIME?

33. Які механізми захисту повинні бути реалізовані для забезпечення функцій захисту інформації на окремих вузлах системи електронних платежів.

34. Опишіть набір функцій, реалізованих в смарт-картці.

Рекомендована література: [3, 4, 5, 6]

ПИТАННЯ ДО ЗАЛІКУ

1. Поняття інформації, інформації з обмеженим доступом, секретної інформації, конфіденційної інформації.
2. Поняття захисту інформації.
3. Національна система конфіденційного зв'язку.
4. Еталонна модель OSI.
5. Базові загальноприйняті послуги безпеки Стандартів ISO 7498, ISO/IEC 10181.
6. Спеціальні механізми забезпечення безпеки зв’язку.
7. Суть механізму нотаризації.
8. Цифровий підпис та цифрова автентифікація.
9. Суть механізму управління маршрутизацією.
10. Послуга управління доступом.
11. Основні приклади послуг безпеки.
12. Приклади основних систем і протоколів захисту інформації на прикладному, сеансовому і мережевому рівнях моделі ВВС.
13. Класифікація порушників.
14. Методи отримання паролів.
15. Стратегії вибору паролів.
16. Підходи до розв’язання проблеми виявлення порушників.
17. Розподілена система виявлення порушень.
18. Алгоритм створення повідомлення системою PGP.
19. Алгоритм отримання повідомлення системою PGP.
20. Загальний формат повідомлення PGP.
21. Алгоритм визначення ступеня довіри ключам.
22. Загальні процедури підготовки повідомлень S/MIME.
23. Система електронних платежів.
24. Смарт-картка. Набір основних функцій, реалізованих в смарт-картці.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА:

1. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – К.: Укр. НДІССІ, 1997. – 11 с.
2. Величко В.В. Передача данных в сетях мобильной связи третьего поколения / В.В.Величко. – М.: Радио и связь, Горячая линия-Телеком, 2005. – 332 с.
3. Горбенко І.Д., Горбенко Ю.І., Прикладна криптологія. Теорія. Практика. Застосування: монографія. – Х.:Видавництво «Форт», 2012, 870 с.
4. Захист інформації в комп'ютерних системах та мережах : навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251с.
5. Мафтик С. Механизми защиты в сетях ЭВМ: пер. с англ. – М.: Мир, 1993. – 216 с.
6. Спесивцев А.В.Защита информации в персональных ЭВМ / А.В. Спе-сивцев, В.А. Вегнер, А.Ю. Крутяков и др. – М.: Радио и связь. МП "Веста", 1993. – 192 с.
7. Стенг Д. Секреты безопасности сетей / Д. Стенг, С. Мун. – К.: Диалектика, 1995. – 544 с.
8. Столингс. В. Криптография и защита сетей. Принципы и практика / В. Столингс. – М.: «Вильямс», 2001. – 672 с.