КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра програмної інженерії та кібербезпеки

ЗАТВЕРДЖЕНО
вченою радою
(пост. 10 п. 10 від "21" червня 2018 р.)
Ректор
_____ А.А. Мазаракі

БЕЗПЕКА ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ / TELECOMMUNICATION NETWORK SECURITY

ПРОГРАМА ТА РОБОЧА ПРОГРАМА / CURRICULUM AND SYLLABUS

освітній ступінь	**магістр /** master
галузь знань	**12 Інформаційні технології /** Information Technology
спеціальність	**121 Інженерія програмного забезпечення /** Software Engineering
спеціалізація	**Інженерія програмного забезпечення /** Software Engineering

Київ 2018

Автор: В.І. Пашорін, канд.техн.наук, проф.

Програму розглянуто і затверджено на засіданні кафедри програмної інженерії та інформаційних систем систем 15 травня 2018 р., протокол №26.

Рецензенти: Рзаєва С. Л., канд. техн. наук, доц.,
Шестак Я. І., директор ІОЦ ГЦІТ КНТЕУ

БЕЗПЕКА ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ / TELECOMMUNICATION NETWORK SECURITY

ПРОГРАМА ТА РОБОЧА ПРОГРАМА/ CURRICULUM AND SYLLABUS

освітній ступінь	**магістр /** master
галузь знань	**12 Інформаційні технології /** Information Technology
спеціальність	**121 Інженерія програмного забезпечення /** Software Engineering
спеціалізація	**Інженерія програмного забезпечення /** Software Engineering

Автор: ПАШОРІН Валерій Іванович

Редактор
Комп'ютерна верстка

Підп. до друку _____. Формат 60x84/16. Папір письм.
Ризографія. Ум. друк. арк. . Ум. фарбо-відб. .
Обл.-вид. арк. . Тираж пр. Зам. .

Центр підготовки навчально-методичних видань КНТЕУ02156, Київ-156, вул. Кіото, 19

ВСТУП

Входження України у світовий інформаційний простір зумовлює швидке впровадження новітніх досягнень комп'ютерних і телекомунікаційних технологій. Системи телекомунікацій активно впроваджуються у фінансові, промислові, торгові і соціальні сфери. У зв'язку з цим різко зріс інтерес широкого кола користувачів до проблем захисту інформації. Захист інформації - це сукупність організаційно-технічних заходів і правових норм для попередження заподіяння збитку інтересам власника інформації. Комунікаційні засоби стали невід'ємною складовою життя людей у всіх сферах діяльності. Мобільні телефони, комп'ютери та Інтернет, розширивши комунікаційні, просторові й часові межі, розкрили нові можливості для спілкування, освіти, праці, відпочинку та творчої самореалізації особистості.

Дисципліна «Безпека телекомунікаційних мереж» розкриває питання законодавства України та світу про захист інформації в телекомунікаційних системах, основи технічного захисту інформації в телекомунікаційних системах, методи та системи криптографічного захисту інформації в телекомунікаційних системах

Основними формами освітнього процесу при викладанні дисципліни «Безпека інтернет-ресурсів» є аудиторні заняття (лекційні та лабораторні), які проводяться в комп'ютерних класах університету та самостійна робота, що виконується індивідуально за допомогою персональних комп'ютерів. Розподіл аудиторних годин за видами робіт визначається навчальними планами КНТЕУ.

Програма містить наступні розділи:

1. Мета, завдання та результати вивчення дисципліни (компетентності), її місце в освітньому процесі.
2. Зміст дисципліни.
3. Структура дисципліни та розподіл годин за темами (тематичний план).
4. Тематика та зміст лекційних та лабораторних занять, самостійної роботи студентів.
5. Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ (КОМПЕТЕНТНОСТІ), ЇЇ МІСЦЕ У ОСВІТНЬОМУ ПРОЦЕСІ

Метою викладання дисципліни є формування теоретичних знань та практичних навичок необхідних для безпечної роботи в телекомунікаційних мережах.

Предметом вивчення дисципліни є вивчення основних положень і принципів, покладених в безпеку функціонування телекомунікаційних мереж , та програмних і технічних засобах що їх реалізують.

Задачі вивчення дисципліни полягають у тому, щоб ознайомити студентів і надати їм навички в роботі по установці, настройці, експлуатації і підтримки в працездатному стані системи захисту телекомунікаційних мереж і безпечній роботі при використані глобальних мереж.

В результаті вивчення дисципліни студент повинен:

Знати:
- вимоги нормативних документів України по безпеці в глобальних мережах;
- основні положення, організацію та моделі систем захисту телекомунікаційних мереж;
- класифікацію атак на інтернет-ресурси та міри протидії;
- технологію та правила мережевої аутентифікації ресурсів і користувачів;
- організацію і правила безпеки при роботі в глобальних мережах;
- технологію та правила експлуатації міжмережевих екранів;
- основи технології віртуальних захищених мереж VPN;
- основи забезпечення захисту в мережевих протоколах передачі.

Уміти:
- визначати загрози в телекомунікаційних мережах;
- організувати захищений видалений доступ до інтернет-ресурсів;
- аналізувати захищеність мереж;
- встановлювати і налагоджувати міжмережеві екрани;
- реєструвати порушення режиму безпеки і складати звіти;
- створювати захист за допомогою програмних засобів;
- організовувати безпечну роботу в глобальних мережах;
- використовувати VPN-рішення для побудови захищених мереж;
- управляти засобами безпеки.

Вивчення дисципліни передбачає використання наступних видів занять: лекції, лабораторні роботи (в комп'ютерному класі на ПК), самостійна робота студенті. Підсумковий контроль проводиться у формі екзамену.

Місце дисципліни в освітньому процесі. Для опанування цією дисципліною за програмою достатньо знань, отримання яких передбачено у програмах Університету з вивчення дисциплін: «Вища математика», «Алгоритмізація та програмування», «Безпека програм та даних», «Методи і засоби захисту інформації в комп'ютерних системах».

2. СТРУКТУРА ДИСЦИПЛІНИ ТА РОЗПОДІЛ ГОДИН ЗА ТЕМАМИ (ТЕМАТИЧНИЙ ПЛАН)

Назва теми	*Кількість годин*				*Форми контролю*
	Усього годин/кредитів	*За формами занять*			
		Лекції	*Лабораторні заняття*	*Самостійна робота студентів*	
Тема 1. *Основи безпеки інформації в телекомунікаційних мережах*	12	2	4	32	УО ІЗ
Тема 2. *Технології безпеки на основі фільтрації та моніторингу мережевого трафіку*	12	4	8	48	УО Пр
Тема 3. *Протоколи захисту в телекомунікаційних мережах*	70	4	8	28	УО, ІЗ, Пр
Тема 4. *Передавання інформації через захищені мережі*	14	2	4	8	УО, ІЗ, Пр
Тема 5. *Забезпечення безпеки взаємодії в телекомунікаційних мережах*	36	2	4	8	ІЗ, Пр
Разом	**180/6**	**14**	**28**	**138**	
Підсумковий контроль семестру - екзамен					

Умовні позначення:

УО – усне опитування ІЗ – перевірка індивідуальних завдань

ПО – письмове опитування Т – тестування

Пр. – презентація індивідуального завдання

3. ТЕМАТИКА ТА ЗМІСТ ЛЕКЦІЙНИХ, ЛАБОРАТОРНИХ ЗАНЯТЬ, САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

Результати навчання	***Навчальна діяльність***	***Робочий час студента год***	***Оцінювання у балах*** *
1	**2**	**3**	**4**
SoftSkills: комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент	**Тема 1.** *Основи безпеки інформації в телекомунікаційних мережах*		
Знати: основні положення, організацію та моделі систем захисту інтернет-ресурсів; класифікацію атак на інтернет-ресурси та міри протидії	**Лекція 1. План лекції** 1. Мережева безпека: терміни та визначення 2. Архітектури захищених мереж. 3. Стандарти безпеки мереж і їх компонентів. 4. Класифікація мережевих загроз **Література** Основна: 2, 3, 4 Додаткова: 10, 11	2	
Знати: вимоги нормативних документів України по безпеці в глобальних мережах	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції з питань: 1. Нормативні документи по безпеці в глобальних мережах 2. Технології виявлення віддалених атак	4	2
Вміти: здійснювати моніторинг існуючих мережевих з'єднань і відкритих портів у комп'ютерній мережі	**Лабораторна робота № 1** *Засоби мережного аудиту* Завдання на лабораторну роботу: 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2.Запустити утиліту TCPView. Ознайомтеся з	4	8

1	2	3	4
	основними пунктами меню 3. Занести до протоколу результати сканування відкритих з'єднань 4. Відкрийте утиліту XSpider. Вивчіть основні пункти меню, скориставшись документацією з меню «Довідка» 5. Запустити програму сканування 6. Виконати сканування по окремих сервісах 7. Проаналізуйте результати сканування вашого завдання. Занесіть до звіту результат сканування. 8. Занесіть до звіту порівняльну характеристику, отриманих вами результатів за допомогою утиліт TCPView і XSpider		
SoftSkills: комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент	**Тема 2.** *Технології безпеки на основі фільтрації та моніторингу мережевого трафіку*		
Знати: технологію та правила експлуатації міжмережевих екранів	**Лекція 2. План лекції** 1. Фільтрація трафіку. Фільтрація Web-змісту (WCF) 2. Віртуальні локальні мережі (VLAN). Технологія перетворення мережевих адрес (NAT) 3. Міжмережеві екрани (МЕ): класифікація та функції МЕ **Література:** Основна: 2-7 Додаткова: 10	2	
	Самостійна робота студентів Вивчення та доповнення матеріалу лекції: 1. Варіанти виконання МЕ 2. Персональні і розподілені мережеві екрани 3. Основні схеми підключення МЕ	12	4
Знати: технологію та правила експлуатації міжмережевих	**Лекція 3. План лекції** 1. Схеми мережевого захисту на базі МЕ 2. Довірена мережа та DMZ мережі **3.** Формування політики міжмережевої взаємодії	2	

1	2	3	4
екранів	**Література:** Основна: 2-7 Додаткова: 8,9,10		
	Самостійна робота студентів Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Проблеми безпеки МЕ 2. Інтерфейс та функціональні можливості програми Outpost Firewall.	12	4
Вміти: встановлювати і налагоджувати міжмережеві екрани	**Лабораторна робота № 2** *Організація мережевої безпеки за допомогою міжмережевого екрана Outpost Firewall* **Завдання на лабораторну роботу:** 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Запустити програму Outpost Firewall. Вивчите функціональні можливості вкладок контекстного меню «Параметри» 3. Налаштувати функції програми Outpost Firewall, залежно від вимог, зазначених у варіанті 4. Налаштувати журнал програми Outpost Firewall, для відображення тільки необхідної інформації, обумовленої завданням 5. Підготувати звіт за результатами роботи програми й виконаними налаштуваннями	4	8
Вміти: аналізувати захищеність інтеренет-ресурсів та виявляти атаки на них	**Лабораторна робота № 3** *Організація мережевої безпеки при використанні засобів виявлення мережевих атак* **Завдання на лабораторну роботу:** 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Запустити утиліту APS, для виявлення факту сканування портів по протоколах TCP, UDP і розсилання UDP broadcast пакетів для заданих портів 3. Налаштувати утиліту APS за наданим варіантом 4. Налаштувати системи імітації сервісів TCP 5. Підготувати звіт за результатами роботи програми й виконаними налаштуваннями	4	8

1	2	3	4
SoftSkills: комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент	**Тема 3.** *Протоколи захисту в телекомунікаційних мережах*		
Знати: основи забезпечення захисту в мережевих протоколах передачі	**Лекція 5. План лекції** 1. Протоколи формування захищених каналів на сеансовому рівні (протоколи SSL/TLS, SOCKS) 2. Захист інтернет-ресурсів на мережевому рівні (протокол IPSec) 3. Особливості реалізації засобів IPSec 4. Протоколи захисту у безпроводових мережах **Література:** Основна: 2,4,5,6 Додаткова: 9,12	4	
	Самостійна робота студентів Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Стандарт мережі з підвищеною безпекою WPA2 2. Основні схеми застосування IPSec	4	2
Вміти: організовувати безпечну роботу в глобальних мережах	**Лабораторна робота 4** *Організація шифрування трафіку при використанні утиліти IPSec* **Завдання на лабораторну роботу:** 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Запустити консоль керування IPSec на комп'ютері 3. Створити свій список фільтрів, зазначений, залежно від варіанта 4. Створити власну дію фільтра, зазначену, залежно від варіанта 5. Створити свою політику IPSec 6. Додати до створеної політики, правило за зазначеними критеріями, залежно від варіанта 7. Підготувати звіт про виконання лабораторної роботи	4	8

1	2	3	4
Вміти: розробляти індивідуальні системи управління доступом і захистом інтернет-ресурсів	**Лабораторна робота 5** *Організація безпеки механізму мережевої автентифікації* **Завдання на лабораторну роботу:** 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Встановити та запустити програму . Cain&Abel. Ознайомитись з можливостями основних пунктів меню програми 3. Виконати сканування MAC-адрес робочих станцій у локальній мережі 4. Виконати завдання за варіантом 5. Підготувати звіт про виконання лабораторної роботи	4	8
SoftSkills: комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики.	**Тема 4.** *Передавання інформації через захищені мережі*		
Знати: основи технології віртуальних захищених мереж VPN	**Лекція 4. План лекції** *Концепція побудови віртуальних приватних мереж VPN* 1. Основні поняття і функції мережі VPN 2. Варіанти побудови віртуальних захищених каналів 3. Класифікація мереж VPN 4. Основні варіанти архітектури VPN **Література:** Основна: 3,4,5 Додаткова: 9,10	2	
	Самостійна робота студентів Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Засоби забезпечення безпеки VPN Методи вкладення інформації у комп'ютерні файли 2. VPN-рішення для побудови захищених мереж	8	2
Вміти: використовувати VPN-рішення для побудови	**Лабораторна робота 6** *Організація мережевої безпеки при використанні засобів VPN* **Завдання на лабораторну роботу:**	4	8

1	2	3	4
захищених мереж; захищати за допомогою програмних засобів	1. Встановити та підготувати віртуальну машину з ОС Windows 7 для виконання лабораторної роботи 2. Використовуючи **Центр управления сетями и общим доступом** створити нове з'єднання і налаштувати VPN тунель 3. Встановити та підготувати віртуальну машину з ОС Windows 10 для виконання лабораторної роботи 4. Використовуючи аплет **Мережі та Інтернет** створити VPN підключення 5. Встановити та налаштувати VPN –сервіс за варіантом 6. Підготувати звіт про виконання лабораторної роботи		
SoftSkills: комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики.	**Тема 5.** *Забезпечення безпеки взасмодії в телекомунікаційних мережах*		
Знати: організацію і правила безпеки при роботі в глобальних мережах	**Лекція 7. План лекції** 1. Управління мережевою ідентифікацією і доступом 2. Організація захищеного віддаленого доступу 3. Протоколи автентифікації віддалених користувачів 4. Централізований контроль віддаленого доступу. Система Kerberos. **Література:** Основна: 5,6 Додаткова: 8,9	2	
	Самостійна робота студентів Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Засоби аналізу захищеності мережевих протоколів і сервісів	8	8
Вміти: створювати захист за допомогою програмних засобів; організовувати безпечну роботу в	**Лабораторна робота 7** **Завдання на лабораторну роботу:** 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Встановити та запустити програму *ESET Smart Security.* Ознайомитись з можливостями основних пунктів меню	4	8

1	2	3	4
глобальних мережах	програми 3. Виконати налаштування сервісів програми за варіантом 4. Підготувати звіт про виконання лабораторної роботи		
Разом за семестр		***180***	***100***

* *Всі лабораторні завдання виконуються на основі інтерактивних методів навчання у комп'ютерному середовищі*

4. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99
2. *Остапов С.Е., Євсеєв С.П., Король О.Г., Технології захисту інформації. Навчальний посібник Чернівці.- Видавничий дом «Родовід», 2017. – 471с.*
3. Кавун С.В. Інформаційна безпека. Навчальний посібник Харків: ХНЕУ, 2016. -213с.
4. Гончарова Л.Л. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. / Л.Л. Гончарова, А.Д. Возненко, О.І. Стасюк, Ю.О. Коваль – К., 2015. – 435 с., іл.160.
5. *Зубок М. І. Інформаційна безпека : Навчальний посібник для студентів вищих навч.закладів / М. І. Зубок. – К. : КНТЕУ, 2009. – 132с.*
6. *КавунС. В. Інформаційна безпека підручник / С. В. Кавун. – Харків : ХНЕУ, 2016. – 368с.*
7. Єсін В. І. Безпека інформаційних систем і технологій : навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2015. – 632с.

Додатковий

8. Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року №2171-111.
9. Інструкція про порядок обліку і зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави від 27 листопада 1998 року № 1893.
10. Положення про порядок здійснення криптографічного захисту інформації в Україні від 22 травня 1998 року № 505/98.
11. *Кормич Б. А. Інформаційна безпека:організаційно-правові основи: навч. посібник для студентів вузів / Б. А. Кормич. – К. : Кондор, 2015. – 384с.*
12. *Пашкова А. Т. Інформаційна безпека як складова національної безпеки А. Т. Пашкова // Безпека життєдіяльності. – Київ, 2014. – № 11. – С. 34-36.*
13. *Полянська В. Кібернетична безпека України в умовах розвитку глобальної інформаційної системи / В. Полянська // Підприємництво, господарство і право. – Київ, 2013. – № 7 (211). – С. 48-50.*

Internet-ресурси

14. Защита информации – режим доступу: *http://www.bseu.by/it/tohod/lekcii9_2.htm*

15. Захист інформації – режим доступу: *http://www.warning.dp.ua/tel28.htm*

16. Безпека на прикладному рівні – режим доступу: *http://www.dut.edu.ua*

* Курсивом виділені назви видань, які знаходяться в бібліотеці КНТЕУ.