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

СИЛАБУС

БЕЗПЕКА ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ / TELECOMMUNICATION NETWORK SECURITY

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

Гарант освітньо-професійної програми "Інженерія програмного забезпечення" другого (магістерського) рівня вищої освіти

Завідувач кафедри програмної інженерії та кібербезпеки, д.т.н., проф. Кривонос О.В.

Київ 2019

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

Силабус розглянуто і затверджено на засіданні кафедри програмної інженерії та інформаційних технологій 10 вересня 2018 р., протокол № 3.

СИЛАБУС
БЕЗПЕКА ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ / TELECOMMUNICATION NETWORK SECURITY

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

1. **Викладач**:

1.1.Лектор: Пашорін Валерій Іванович

- *вчене звання та посада*: канд техн. наук, професор, професор кафедри програмної, інженерії та кібербезпеки;
- *педагогічний стаж* – 20 років;
- *контактний телефон:* (044)-531-49-56;
- *e-mail:* vpashorin@gmail.com
- *наукові інтереси*: безпека інформацйних систем, операційні системи, комп'ютерні мережі
- *стажування та підвищення кваліфікації*: Проходив підвищення кваліфікації в Центрі сертифікаційного навчання «ПРОКОМ» (м. Київ, сертифікати по різним модулях «1С: Підприємство» в 2017р.

2. **Дисципліна**: «**Безпека телекомунікаційних мереж**»,
   - рік навчання: II;
   - семестр навчання: III;
   - кількість кредитів: 6;
   - кількість годин за семестр: 180 год.
     - лекційних: 14 год.
     - лабораторних: 28 год.
     - на самостійне опрацювання: 138 год.
   - кількість аудиторних годин на тиждень:
     - лекційних: 2 год.
     - лабораторних: 4 год.

3. **Час та місце проведення:**
   - аудиторні заняття - відповідно до розкладу КНТЕУ з врахуванням специфіки дисципліни проведення останньої передбачено в аудиторіях: 504, 510, 510а, 514;
   - поза аудиторна робота - самостійна робота студента, результат виконання якої висвітлено засобами Office 365;
   - всі лабораторні завдання виконуються на основі інтерактивних методів навчання у електронному середовищі. Передбачається можливість проведення лабораторних та лекційних занять на базах підприємств-партнерів.

4. **Пререквізити та постреквізити навчальної дисципліни:**
   - **пререквізити:** 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».

– **постреквізити:** 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.

5. Характеристика дисципліни:

Призначення навчальної дисципліни: 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

5.1. Мета вивчення дисципліни: викладання дисципліни є формування теоретичних знань та практичних навичок необхідних для безпечної роботи в телекомунікаційних мережах.

5.2. 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.

5.3. Зміст навчальної дисципліни: відповідає навчальній та робочій програмі, яка відповідає запитам стейкхолдерів.

5.4. План вивчення дисципліни

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 основними пунктами меню 3. Занести до протоколу результати сканування	4	8

1	2	3	4
	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 екранів	**Лекція 3. План лекції** 1. Схеми мережевого захисту на базі МЕ 2. Довірена мережа та DMZ мережі **3.** Формування політики міжмережевої взаємодії **Література:** Основна: 2-7 Додаткова: 8,9,10	2	
	Самостійна робота студентів Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Проблеми безпеки МЕ 2. Інтерфейс та функціональні можливості	12	4

1	2	3	4
	програми Outpost Firewall.		
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
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	**Лекція 5. План лекції** 1. Протоколи формування захищених каналів на сеансовому рівні (протоколи SSL/TLS, SOCKS) 2. Захист інтернет-ресурсів на мережевому рівні	4	

1	2	3	4
протоколах передачі	(протокол IPSec) 3. Особливості реалізації засобів IPSec 4. Протоколи захисту у безпроводових мережах **Література:** Основна: 2,4,5,6 Додаткова: 9,12		
	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
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	**Тема 4.** *Передавання інформації через захищені мережі*		

1	2	3	4
навички, сприйняття конструктивної критики.			
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 захищених мереж; захищати за допомогою програмних засобів	**Лабораторна робота 6** *Організація мережевої безпеки при використанні засобів VPN* **Завдання на лабораторну роботу:** 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	4	8
SoftSkills: комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики.	**Тема 5.** *Забезпечення безпеки взасмодії в телекомунікаційних мережах*		

1	2	3	4
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 глобальних мережах	**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 програми 3. Виконати налаштування сервісів програми за варіантом 4. Підготувати звіт про виконання лабораторної роботи	4	8
Разом за семестр		***180***	***100***

6. 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.

7. **Контроль та оцінювання результатів навчання:** положення про оцінювання результатів навчання студентів і аспірантів наказ КНТЕУ №2891 від 16.09.2019р.

Під час вивчення дисципліни «Хмарні та GRID-технології» викладачем здійснюється поточний та підсумковий контроль. Поточний контроль та оцінювання передбачає:

- перевірку рівня засвоєння теоретичного матеріалу (тестування за матеріалами лекції, який здійснюється на початку кожної наступної лекції з використанням 365 Office);
- захист лабораторних робіт (проходить під час наступної лабораторної роботи);
- перевірка засвоєння матеріалу, що винесений на самостійне опрацювання під час фронтального опитування на лекції.

8. Політика навчальної дисципліни:

8.1. Відвідування лекційних та лабораторних занять: відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).

8.2. Відпрацювання пропущених занять: відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).

8.3. Правила поведінки під час занять: обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем).

8.4. За порушення академічної доброчесності студенти будуть притягнені до академічної відповідальності у відповідності до положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти КНТЕУ (Наказ КНТЕУ від 02.02.2018 №377).