Міністерство освіти і науки України
Дніпропетровський національний університет залізничного транспорту імені академіка В. Лазаряна

Факультет «Технічна кібернетика»
Кафедра «Електронні обчислювальні машини»

ЗАТВЕРДЖУЮ
Завідувач кафедри ЕОМ
професор _____ І. В. Жуковицький
«30» 05 2018 р.

Безпека інформаційних технологій та систем

РОБОЧА ПРОГРАМА
навчальної дисципліни
для здобувачів ступеня «доктор філософії»
із галузей та спеціальностей

12 Інформаційні технології 122 Комп'ютерні науки

Розробник робочої програми, _____ проф. Жуковицький І.В.

Декан факультету ТК _____ проф. Скалозуб В.В.

Начальник навчального відділу _____ Андрашко Л.Є.

м. Дніпро – 2018

Робоча програма з дисципліни *Інформаційна безпека*

Ухвалено на засіданні кафедри «22» 05 2018 р., протокол № 10

Зав. кафедри ЕОМ, проф. _____ Жуковицький І.В.

Лектор, проф. _____ Жуковицький И.В.

Доповнення/зміни до робочої програми

На 2019/2020 н.р._____

Зміни теми лекцій, Лекція 10 – IPS

Лекція 11 – IPS

«30» 09 2019 р. протокол № 1 Зав. кафедри _____

Лектор _____

На 20___/20___ н.р._____

«__» __ 20_ р. протокол № ___ Зав. кафедри _____

Лектор _____

1 Розподіл навчального часу для денної форм навчання
2018 / 2019 навчальний рік

Види навчання	Усього				Усього	
	другий семестр*					
	I половина		2 половина			
	ак. год	кр ECTS	ак. год	кр ECTS	ак. год	кр ECTS
Усього годин за навчальним планом	60	2	60	2	120	4
у тому числі: **Аудиторні заняття**	27		27		54	
з них: - лекції	18		18		36	
- лабораторні заняття						
- практичні заняття	9		9		18	
- семінарські заняття	-		-		-	
Самостійна робота	34		37		66	
у том числі при: підготовці до лекції	9		9		18	
- підготовці до практичних робіт	4,5		4,5		9	
- опрацювання розділів програм, які не викладаються на лекціях					39	
- підготовка до контрольних заходів та їх складання						
Підсумковий контроль					залік	

Примітки: - нумерація семестрів наскрізна

2 Зміст дисципліни

Лекції

№№ теми	Назва розділу/теми та її зміст	Години
1	**Вступ.** Сучасна ситуація в області інформаційної безпеки. Категорії інформаційної безпеки згідно стандартам. Абстрактні моделі захисту інформації. Огляд найбільш розповсюджених методів "злому": криптоаналіз, трояни, сніфінг, людина посередині, тощо.	2
2	**Огляд основних механізмів захисту інформації** Обмеження доступу, криптографічний захист, мережевий захист. Основні механізми ідентифікації та аутентифікації: парольний захист, біологічні ознаки, токени. Механізми доступу до інформаційних систем: деклараційний, мандатний. Мітка об’єкту, мітка суб’єкту.	2
3	**Криптографія, її джерела та місце в сучасному суспільстві** Задачі, що вирішуються криптографічними методами. Модель інформаційного обміну з порушником. Основні терміни криптографії. Алгоритми побудови базових симетричних шифрів. Шифри перестановки. Шифри підстановки. Типові симетричні шифри: Шифр Цезаря. Шифр Веженара. Одноразовий блокнот.	2
4	**Крипостійкість симетричних шифрів** Невизначеність повідомлень по Шеннону. Абсолютно стійкий шифр – необхідні умови. Реальні абсолютно стійки шифри.	2
5	**Основи побудови блочних шифрів. Мережа Фейштеля** Поняття блочного шифру. Типові елементи блочного шифру Нелінійні перетворення. Поняття інваріанту. Реалізація інваріанту. Стандартне шифруючи перетворення. Узагальнена мережа Фейштеля.	2
6	**Сучасні симетричні шифри** Узагальнена структура та параметри шифру DES, ГОСТ 28147-8, AES Структура раундів. Елементи шифруючих перетворень	2

7	**Основи асиметричних криптосистем** Односторонні функції. Односторонні функції з секретом. Теорема Ейлера. Загальна структура криптографічної системи з відкритим ключем. Загальна послідовність зашифрування/розшифрування в цієй системі. Математичній опис та алгоритм формування пари ключів RSA. Зашифрування/розшифрування повідомлення по алгоритму RSA	2
8	**Електронний цифровий підпис (ЕЦП)** Вимоги до ЕЦП. ЕЦП за стандартом RSA: математичні основи, алгоритми. Призначення сертифікатів. Механізм сертифікації. Дерево центрів сертифікації. Міжнародний стандарт сертифікації. Особливості сертифікації згідно вітчизняного стандарту	2
9	**Типові мережеві атаки** Класифікація видалених атак на розподілені обчислювальні системи. Характеристика і механізм реалізації типових видалених атак: Аналіз мережевого трафіку, підміна довіреного об'єкта або суб'єкта розподіленої ОС, помилковий об'єкт розподіленої ОС, відмова в обслуговуванні.	2
10	**Питання безпеки протоколу TCP/IP** Сніффінг. Пасивний сніффінг скрізь концентратор. Активний сніффінг скрізь комутатор. Захист від прослуховування. Сканування портів. Види сканування за допомогою програми Nmap. Захист від сканування.	2
11	**Питання безпеки протоколу TCP/IP** Перехват даних. Використання недоліків алгоритму вилученого пошуку. Помилковий ARP-сервер. Помилковий DNS-сервер у мережі Internet.. Нав’язування хосту помилкового маршруту за допомогою ICMP для створення в мережі помилкового маршрутизатора. Атака «Відмова в обслуговуванні». Захист від цього роду атак.	2

12	**Захищені віртуальні мережі (VPN). Тунелювання на канальному рівні** Протокол PPTP, як розширення протоколу PPP. Структура пакету PPTP. Схеми застосування протоколу PPTP: пряме з'єднання комп'ютера віддаленого користувача із Internet та два випадка підключення віддаленого комп'ютера до Inetrnet по телефонній лінії скрізь провайдера. Особливості протоколу L2F. Схема взаємодії по протоколу L2F. Особливості протоколу L2TP. Схема взаємодії по протоколу L2TP.	2
13	**Побудова захищених віртуальних мереж на мережевому рівні** Архітектура засобів безпеки IPSec. Архітектура IPsec. Поняття асоціації безпеки IPSec. Режими IPSec. Випадки асоціацій (огляд). Протокол аутентифікації AH (Authentication Header): заголовок аутентифікації, код контролю цілісності, транспортний і тунельний режими. Протокол шифрування (Encapsulation Security Payload). Поля заголовка в транспортному і тунельному режимах Керування захищеним тунелем	2
14	**Побудова захищених віртуальних мереж на сеансовому рівні** Особливості тунеліювання на сеансовому рівні. Протокол SSL - сімейство протоколів. Призначення SSL. Архітектура SSL. Поняття сеансу SSL, з'єднання SSL. Протокол запису SSL. Загальна схема роботи протоколу запису SSL. Формат запису SSL. Протокол зміни параметрів шифрування. Протокол повідомлення. Протокол квитування. Схема роботи протоколу квитування. Побудова ключів шифрування SSL. Протокол TLS – наступна версія протоколу SSL. Основні схеми захисту на основі Firewall: Firewall - маршрутизатор з фільтрацією пакетів, Firewall на основі шлюзу, екранований шлюз, Firewall - екранована під мережа, об'єднання модемного пула з Firewall. Особливості захисту мереж на основі Firewall: етапи розробки політики доступу до служб, гнучкість політики, забезпечення Firewall, адміністрування Firewall.	6

Практичні заняття

1	Налаштування пакетних фільтрів з використання програми ipfw і спостереження за результатами їх роботи	4
2	Використання internet protocol security (ipsec) для захисту конфіденційних даних, які передаються по протоколу tcp / ip	4
3	Віддалений доступ до мережі з використанням віртуального захищеного з'єднання pptp і l2tp	4
4	Використання протоколу ssl для безпечного взаємодії клієнтів з веб-сервером iis	6

3 Методи навчання

Лекції з використанням електронних дидактичних демонстраційних матеріалів (презентації), що призначені для супроводу навчального процесу.

Лабораторні заняття з використанням відповідного лабораторного обладнання (локальна мережа, відповідне програмне та методичне забезпечення)

Самостійна робота з використанням друкованих та електронних підручників, можливості локальної мережі та Інтернет.

Методи контролю.

Методами контролю успішності навчання є співбесіда за програмою курсу

4 Діагностування рівня успішності

Діагностування знань здійснюється письмовим контролем з набору тестових питань за змістом лекційного матеріалу та результатами виконання (з усним опитуванням) лабораторних робіт. Кількість балів на кожну відповідь з набору тестових питань та за з тем лабораторних занять зазначається з урахуванням їх складності, обсягу та значущості в засвоєнні дисципліни:

Оцінка			**Рівень компетентності**
ECTS	**бали**	**національна**	
1	2	3	4
A	90-100	5	**Вищий рівень компетентності:** - аспірант глибоко і в повному обсязі засвоїв програмний матеріал, грамотно, вичерпно та логічно викладає його в усній або письмовій формі, знає рекомендовану літературу, виявляє творчий підхід і правильно обґрунтовує прийняті рішення, добре володіє різносторонніми уміннями та навичками при виконанні практичних задач, відмінно виконує текстові та графічні матеріали
B	82-89	4	**Високий рівень компетентності:** - аспірант знає програмний матеріал, грамотно і за суттю викладає його в усній або письмовій формі, припускаючи незначні помилки у доказах, трактовці понять та категорій; при цьому володіє необхідними уміннями та навичками при виконанні практичних задач, відмінно виконує текстові та графічні матеріали, мають місце деякі помарки
C	75-81	4	**Середній рівень компетентності:** - аспірант знає програмний матеріал, грамотно викладає його в усній або письмовій формі, припускаючи неточності в доказах, трактовці понять та категорій; при цьому володіє необхідними уміннями та навичками при виконанні практичних задач, добре виконує текстові та графічні матеріали

1	2	3	4
D	67-74	3	**Достатній рівень компетентності:** - аспірант знає тільки основний програмний матеріал, припускає неточності, недостатньо чіткі формулювання, непослідовність у викладанні відповідей в усній або письмовій формі; при цьому невпевнено володіє уміннями та навичками виконання практичних завдань, задовільно виконує текстові та графічні матеріали
E	60-66	3	- аспірант знає тільки основний програмний матеріал, припускає грубі неточності, нечітко формулює і непослідовно дає відповіді в усній або письмовій формі; при цьому невпевнено володіє уміннями та навичками виконання практичних задач, задовільно виконує текстові та графічні матеріали
FX, F	0-59	2	**Недостатній рівень компетентності:** - аспірант не володіє основним програмним матеріалом, допускає грубі помилки, які свідчать про нерозуміння матеріалу, у розрахунках отримані неправильні результати, на запитання дає неправильні відповіді; припускає принципові помилки у доказах, трактовці понять та категорій, не володіє основними уміннями та навичками при виконанні практичних задач, потрібна додаткова навчальна робота з дисципліни
			- аспірант не розуміє і не орієнтується у матеріалі, розрахунки не доводить до кінця, не дає відповіді на запитання; потрібний повторний курс вивчення дисципліни

5 Інформаційно-методичне забезпечення

6 Рекомендована література

Основна

1. Столлингс В. Криптография и защита сетей: принципы и практика. М.: Издательский дом «Вильямс», 2001. – 672с
2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008.
3. Биячуев Т.А. / под ред. Л.Г.Осовецкого Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004.- 161 с.
4. Жуковицький І.В. Прикладна криптографія. Методичні вказівки до лабораторних робіт. Дніпропетровськ, ДІІТ, 2007р.
5. Мотин А.С. Методические указания к лабораторным работам по курсу «Защита информации в компьютерных сетях» (электронный вариант).
6. И.В. Жуковицкий, Д.А. Остапец, С.А. Разгонов, А.П. Заец. Безопасность и резильентность систем и сетей. Харьков, 2017.
7. Secure and resilient computing for Industry and human domains. Secure and resilient Systems, networks and Infrastructures. Kharkov, 2017

Додаткова

6. В.Зима, А.Молдовян, Н.Молдовян. Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2000.
7. Запечников С.В. и др. Основы построения виртуальных частных сетей. Учебное пособие для вузов. М.: Горячая линия-Телеком, 2003.
8. Браун С. Виртуальные частные сети. Издательство «Лори», 2001.
9. Мерит М. Безопасность беспроводных сетей. ДМК Пресс, 2004. – 288с.
10. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ-Петербург, 2003. – 608.

7 Інформаційні ресурси

Навчальні матеріали, розроблені в ході виконання міжнародного пректу SEREIN: https://serein.eu.org/teaching-materials/