Силабус курсу:

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВОЛОДИМИРА ДАЛЯ

МЕРЕЖНА ТА ІНТЕРНЕТ БЕЗПЕКА

Ступінь вищої освіти:	бакалавр
Спеціальність:	122 «Комп'ютерні науки», 123 «Комп'ютерна інженерія»,
Рік підготовки:	2
Семестр викладання:	осінній
Кількість кредитів ЄКТС:	3
Мова(-и) викладання:	українська
Вид семестрового контролю	залік

Автор курсу та лектор:

Лифар Олена Костянтинівна

вчений ступінь, вчене звання, прізвище, ім'я та по-батькові

старший викладач кафедри комп'ютерних наук та інженерії

посада

lyfar_o@snu.edu.ua (електронна адреса) | +38-097-35-55-129 (телефон) | Skype: eklyfar (месенджер) | 401 НК, за розкладом (консультації)

Викладач лабораторних занять:*

Лифар Олена Костянтинівна

вчений ступінь, вчене звання, прізвище, ім'я та по-батькові

старший викладач кафедри комп'ютерних наук та інженерії

посада

lyfar_o@snu.edu.ua (електронна адреса) | +38-097-35-55-129 (телефон) | Skype: eklyfar (месенджер) | 401 НК, за розкладом (консультації)

Викладач практичних занять:*

Лифар Олена Костянтинівна

вчений ступінь, вчене звання, прізвище, ім'я та по-батькові

старший викладач кафедри комп'ютерних наук та інженерії

посада

lyfar_o@snu.edu.ua (електронна адреса) | +38-097-35-55-129 (телефон) | Skype: eklyfar (месенджер) | 401 НК, за розкладом (консультації)

Анотація навчального курсу

Цілі вивчення курсу:

Метою викладання дисципліни “Мережна та інтернет безпека” є вивчення основних методів захисту інформації в комп’ютерних системах та мережах, проведення аналізу основних загроз та вивчення методів боротьби з ними. Створення та супроводження комплексної системи захисту інформації.

Метою лекційних занять за дисципліною «Мережна та інтернет безпека» є забезпечення достатнього рівня теоретичних знань, необхідних для створення та супроводження комплексної системи захисту інформації. Вивчення математичних моделей безпеки, які надають теоретичну базу для побудови сучасних систем захисту інформації.

Метою лабораторних та практичних занять за дисципліною «Мережна та інтернет безпека» є розширення, поглиблення та деталізація теоретичних знань, отриманих студентами на лекціях та в процесі самостійної роботи, прищеплення умінь і навичок з захисту сучасних комп’ютерних технологій обробки інформації, які зорієнтовані на розподільну обробку даних на основі автоматизованих робочих місць, експертних і навчальних систем, локальних і глобальних комп‘ютерних мереж і впровадження інформаційних систем нового покоління – систем підтримки прийняття рішень.

Метою самостійної роботи за дисципліною є систематизація і закріплення отриманих теоретичних знань і практичних навичок студентів; формування вмінь використовувати нормативну і спеціальну літературу; розвиток пізнавальних здібностей.

Курс може бути корисним здобувачам за спеціальностями в галузі знань «12. Інформаційні технології» а також майбутнім менеджерам та перекладачам, що планують працевлаштування на підприємства та фірми діяльність яких пов’язана з інформаційними технологіями.

Результати навчання:

ПР2 Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних.

ПР6 Вміння системного мислення, застосування методології системного аналізу для дослідження складних проблем різної природи, методів формалізації та розв'язанні системних задач, що мають суперечливі цілі, невизначеності та ризики.

ПР14 Знати, вміти, застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти та експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

ПР15 Знання методів, засобів та інформаційних технологій для виявлення несанкціонованого доступу на різних ієрархічних рівнях інформаційно-комунікаційної системи.

ПР17 Застосовувати на практиці програмні засоби, навички

	роботи в телекомунікаційних та комп'ютерних мережах. ПР19 Знати, розуміти, аналізувати, вибирати, кваліфіковано застосовувати засоби безпеки складових інформаційних систем і мереж відповідно до правил експлуатації.
Передумови до початку вивчення:	Базові знання та уявлення дисциплін «Основи ІТінженерії аналізу безпеки комп'ютерних систем», «Адміністрування комп'ютерних мереж», «Захист інформації в комп'ютерних системах», «Комп'ютерні системи та архітектура комп'ютерів»

Мета курсу (набуті компетентності)

В наслідок вивчення даного навчального курсу здобувач вищої освіти набуде наступних компетентностей:

1. ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.
2. ЗК2. Здатність застосовувати знання у практичних ситуаціях
3. ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.
4. ЗК6. Здатність вчитися і оволодівати сучасними знаннями.
5. ЗК8. Здатність генерувати нові ідеї (креативність).
6. ЗК13. Здатність оцінювати та забезпечувати якість виконуваних робіт.
7. ФК3. Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки
8. ФК4. Здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі
9. ФК5. Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем
10. ФК6. Здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов
11. ФК7. Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС
12. ФК10. Здатність здійснювати управління інцидентами інформаційної та кібербезпеки
13. ФК11. Здатність здійснювати управління ризиками інформаційної та кібербезпеки
14. ФК12. Здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій
15. ФК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти та експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

Структура курсу

№	Тема	Години (Л/ЛБ/ПЗ)	Стислий зміст	Інструменти і завдання
1.	Забезпечення захисту інформації в інформаційно-комунікаційних системах.	2/0/2	Базові поняття. Системи, в яких здійснюється захист інформації. Завдання захисту інформації. Комплексна система захисту інформації. Об'єкти захисту та їхні властивості. Загрози безпеці інформації. Класифікація загроз. Класифікація атак. Методика класифікації загроз STRIDE. Порушники. Наслідки від дій порушників.	Участь в обговоренні Тести Індивідуальні завдання
2.	Будова систем захисту інформації.	2/0/2	Рівні інформаційно-комунікаційної системи. Функціональні сервіси безпеки і механізми, що їх реалізують. Таксономія функцій систем захисту, механізми захисту на різних рівнях. Основні підсистеми комплексу засобів захисту: підсистема керування доступом, підсистема ідентифікації й автентифікації, підсистема аудита, підсистема забезпечення цілісності, криптографічна підсистема.	Участь в обговоренні Тести Індивідуальні завдання
3.	Основи криптографічних методів захисту інформації	2/4/2	Історична довідка. Основні поняття криптографії. Шифрування з ключем. Симетричне шифрування: потокове шифрування, блокове шифрування. Асиметричне шифрування. Поняття криптографічної системи.	Участь в обговоренні Тести Індивідуальні завдання
4.	Теоретичні основи захисту інформації.	2/0/2	Загальні поняття теорії захисту інформації. Основні типи політик безпеки. Математичні моделі безпеки. Моделі дискреційної політики безпеки: Модель Харрісона - Руззо – Ульмана, модель Take-Grant. Моделі мандатної політики безпеки: модель конфіденційності Белла – ЛаПадула, модель цілісності Біба.	Участь в обговоренні Тести Індивідуальні завдання
5.	Основні загрози безпеці інформації в інформаційно-комунікаційних системах.	1/0/1	Типові вразливості систем і аналіз причин їх появи. Передумови виникнення вразливостей у комп'ютерних системах. Класифікація вад захисту. Класифікація помилок, що виникають у процесі програмної реалізації системи: помилки контролю припустимих значень параметрів, помилки визначення областей, помилки послідовності дій, помилки ідентифікації й автентифікації, помилки перевірки границь об'єктів.	Участь в обговоренні Тести Індивідуальні завдання
6.	Шкідливе програмне забезпечення	1/4/1	Класифікація шкідливого програмного забезпечення. Програмні закладки. Шпигунські програми, «Логічні бомби». Люки - утиліти віддаленого адміністрування. Несанкціонована робота з мережею. Комп'ютерні віруси: файлові віруси, завантажувальні віруси, макровіруси, скриптові віруси. Захист від комп'ютерних вірусів. Мережні хробаки, їх класифікація. «Троянські коні», їх класифікація.	Участь в обговоренні Тести Індивідуальні завдання
7.	Нормативні документи з оцінювання захищеності інформації	2/0/2	Призначення стандартів інформаційної безпеки. Стандарти, орієнтовані на застосування військовими та спецслужбами. Класи безпеки комп'ютерних систем. Законодавча і нормативна база захисту інформації в Україні.	Участь в обговоренні Тести Індивідуальні завдання
8.	Захист інформації на рівні операційної системи. Захищені	2/0/2	Апаратне забезпечення засобів захисту. Поняття захищеної операційної системи. Підходи до побудови захищених операційних систем.	Участь в обговоренні Тести

№	Тема	Години (Л/ЛБ/ПЗ)	Стислий зміст	Інструменти і завдання
	операційні системи.		Адміністративні заходи захисту, політика безпеки. Типова архітектура комплексу засобів захисту операційних систем.	Індивідуальні завдання
9.	Засоби захисту в операційній системі Windows.	2/4/2	Відповідність вимогам стандартів безпеки. Архітектура системи. Основні концепції. Компоненти системи захисту. Розмежування доступу. Основні принципи реалізації системи розмежування доступу. Стандартні настроювання прав доступу. Реалізація дискреційного керування доступом. Механізми перевірки прав доступу. Аналіз причин уразливостей системи Windows.	Участь в обговоренні Тести Індивідуальні завдання
10.	Системи оброблення конфіденційної інформації	2/0/2	Обґрунтування застосування захищених ОС для створення систем оброблення конфіденційної інформації. Система Trusted Solaris. Основні характеристики середовища Trusted Solaris. Керування доступом у середовищі Trusted Solaris. Окреме зберігання позначеної мітками інформації у середовищі Trusted Solaris. Адміністрування безпеки у середовищі Trusted Solaris. Операційна система Фенікс. Архітектура системи. Засоби захисту. Дискреційна модель ієрархічного керування.	Участь в обговоренні Тести Індивідуальні завдання
11.	Захист інформації в розподілених системах	2/0/2	Основи безпеки інформації в комп'ютерних мережах. Відкриті системи. Модель взаємодії відкритих систем. Стеки протоколів. Інтернет: організація, адресація, IP-адреси в Інтернеті, доменні імена. Маршрутизація. Загрози безпеці інформації у мережах. Безпека взаємодії відкритих систем. Універсальні механізми безпеки. Керування безпекою.	Участь в обговоренні Тести Індивідуальні завдання
12.	Безпека мережних протоколів Інтернету	2/2/2	Протоколи прикладного рівня. Протокол Telnet. Протокол FTP, основні команди. Проблеми з безпекою протоколу FTP. Транспортні протоколи. Протокол UDP. Протокол TCP. Процедура встановлення TCP-з'єднання. Захисні функції TCP. Протокол IP. Призначення й можливості протоколу IPv4. Протокол маршрутизації BGP. Механізми захисту: IPsec, узагальнений механізм безпеки TTL, політики захищеної маршрутизації. Протоколи керування мережею.	Участь в обговоренні Тести Індивідуальні завдання
13.	Безпека прикладних служб Інтернету.	2/0/2	Система електронної пошти. Архітектура системи електронної пошти. Формат повідомлення електронної пошти. Протокол SMTP. Протокол POP3. Протокол IMAP4. Загрози, пов'язані з використанням електронної пошти. Веб-служба. Принципи веб-технології. Протокол HTTP. Захист сервера від атак.	Участь в обговоренні Тести Індивідуальні завдання
14.	Засоби захисту в розподілених інформаційно-комунікаційних системах.	2/0/2	Архітектура захищених мереж. Протидія прослуховуванню трафіку. Сегментація мережі. Резервування мережного обладнання і каналів зв'язку. Міжмережні екрани. Системи виявлення атак. Аналіз подій у системах виявлення атак. Додаткові інструментальні засоби. Системи аналізу й оцінювання вразливостей. Аналіз уразливостей на рівні вузла й мережі. Перевірка цілісності файлів.	Участь в обговоренні Тести Індивідуальні завдання
15.	Передавання інформації	2/0/2	Захист інформації, що передається відкритими	Участь в

№	Тема	Години (Л/ЛБ/ПЗ)	Стислий зміст	Інструменти і завдання
	через захищені мережі.		каналами зв'язку. Віртуальні захищені мережі. Проблеми побудови віртуальних захищених мереж. Забезпечення конфіденційності, цілісності, автентифікація та унеможливлення відмови від авторства. Способи утворення захищених віртуальних каналів. Рівні реалізації віртуальних захищених мереж.	обговоренні Тести Індивідуальні завдання

Рекомендована література

1. Грайворонський М.В., Новіков.О.М., Безпека інформаційно-комунікаційних систем. – Київ: Видавнича група BHV, 2009. – 608 с.
2. Теоретические основы компьютерной безопасности / П. Н. Девянин, О. О. Михальский, Д. И. Правиков, А. Ю. Щербаков. -М.: Радио и связь, 2000. - 192 с.
3. НД ТЗГ 1.1-002-99: Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, №22.
4. 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.
5. . Ховард М., Лебланк Д. Защищенный код / Пер. с англ. — М.: Издательеко-торговый дом «Русская редакция», 2003. - 704 с.
6. Богуш В. М., Кудін А. М. Інформаційна безпека від А до Я. — К.: МОУ, 1999. — 456 с.
7. Диффи У., Хеллмэн М. Защищенность и имитостойкость: Введение в криптографию. // ТИИЭР, 1979, т. 67, № 3. - С. 71-109.
8. Чмора А.Л. Современная прикладная криптография. — М.: Гелиос АРВ, 2001. — 256 с.
9. Мельников В. В. Защита информации в компьютерных системах. - М.: Финансы и статистика; Электроинформ, 1997. — 368 с.
10. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. — М.: «Горячая линия» — Телеком, 2004. — 280 с.
11. Девятин П. Н. Модели безопасности компьютерных систем. — М.: Издательский центр «Академия», 2005. — 144 с.
12. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. - М.: издатель Молгачева С. В., 2001. — 352 с.
13. Корт С. Теоретические основы защиты информации. — СПб.: Издательство Гелиос — АРВ, 2004. - 240 с.

Методичне забезпечення

1. Конспект лекцій з дисципліни «Мережна та інтернет безпека» Для студентів денної і заочної форм навчання напряму підготовки 6.170101 «Безпека інформаційних і комунікаційних систем».” (електронне видання) / Укл. Лифар О.К. -Сєвєродонецьк: вид-во СНУ ім. В.Даля, 2017.– 380с.
2. Методичні вказівки до виконання практичних завдань з дисципліни «Мережна та інтернет безпека» Для студентів денної і заочної форм навчання спеціальності 122 «Комп’ютерні науки». (електронне видання) / Укл. Лифар О.К. -Сєвєродонецьк: вид-во СНУ ім. В.Даля, 2022.

Оцінювання курсу

За повністю виконані завдання студент може отримати визначену кількість балів:

Інструменти і завдання	Кількість балів
Участь в обговоренні	20
Тести	25
Індивідуальні завдання	25
Залік	30
Разом	**100**

Критерії оцінювання та система розподілу балів

Поточний контроль здійснюється лектором. Викладач розробляє чіткі критерії оцінювання всіх видів навчальної роботи у комплексному контролі знань, доводить їх до відома студентів на початку змістовного модулю.

*Система оцінювання аудиторної роботи***.**

Поточна аудиторна діяльність студента оцінюється за чотирибальною (національною) шкалою.

Форми участі студентів у навчальному процесі, які підлягають поточному контролю:

- виступ з основного питання;
- усна доповідь;
- доповнення, запитання до того, хто відповідає, рецензія на виступ;
- участь у дискусіях, інтерактивних формах організації заняття;
- аналіз джерельної та монографічної літератури;
- письмові завдання (тестові, контрольні, творчі роботи, реферати тощо);
- самостійне опрацювання тем;
- підготовка тез, конспектів навчальних або наукових текстів;
- систематичність роботи на семінарських заняттях, активність під час обговорення питань;
- та інші.

Критеріями оцінки є:

1) для усних відповідей:

- повнота розкриття питання;
- логіка викладання, культура мови;
- емоційність та переконаність;
- використання основної та додаткової літератури;
- аналітичні міркування, уміння робити порівняння, висновки ;
- та інші.

2) для виконання письмових завдань:

- повнота розкриття питання;
- цілісність, системність, логічність, уміння формулювати висновки;
- акуратність оформлення письмової роботи
- та інші.

Критерії оцінки рівня знань на практичних заняттях.

На практичних заняттях кожен студент з кожної теми виконує індивідуальні завдання.

Рівень знань оцінюється: ***«відмінно»*** – студент дає вичерпні, обґрунтовані, теоретично і практично правильні відповіді не менш ніж на 90% запитань, рішення задач та вправи є правильними, демонструє знання підручників, посібників, інструкцій, проводить узагальнення і висновки, акуратно оформляє завдання, був присутній на лекціях, має конспект лекцій чи реферати з основних тем курсу;

«добре»– коли студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій і розрахунків, проте за допомогою викладача швидко

орієнтується і знаходить правильні відповіді, був присутній на лекціях, має конспект лекцій чи реферати з основних тем курсу;

«задовільно»– коли студент дає правильну відповідь не менше ніж на 60% питань, або на всі запитання дає

недостатньо обґрунтовані, невичерпні відповіді, допускає грубі помилки, які виправляє за допомогою викладача. При цьому враховується наявність конспекту за темою завдань та самостійність;

«незадовільно з можливістю повторного складання» – коли студент дає правильну відповідь не менше ніж на 35% питань, або на всі запитання дає необґрунтовані, невичерпні відповіді, допускає грубі помилки. Має неповний конспект лекцій. Підсумкова (загальна оцінка) курсу навчальної дисципліни є сумою рейтингових оцінок (балів), одержаних за окремі оцінювані форми навчальної діяльності: поточне та підсумкове засвоєння теоретичного матеріалу

Шкала оцінювання студентів

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ECTS</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>для екзамену, курсового проекту (роботи), практики</td><td>для заліку</td></tr>
<tr><td>90 – 100</td><td>A</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>незадовільно з можливістю повторного складання</td><td>не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-34</td><td>F</td><td>незадовільно з обов’язковим повторним вивченням дисципліни</td><td>не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

Політика курсу

Плагіат та академічна доброчесність: Під час виконання завдань студент має дотримуватись політики академічної доброчесності. Запозичення мають бути оформлені відповідними посиланнями. Списування є забороненим.

Завдання і заняття: Всі завдання, передбачені програмою курсу мають бути виконані своєчасно і оцінені в спосіб, зазначений вище. Аудиторні заняття мають відвідуватись регулярно. Пропущені заняття (з будь-яких причин) мають бути відпрацьовані з отриманням відповідної оцінки не пізніше останнього тижня поточного семестру. В разі поважної причини (хвороба, академічна мобільність тощо) терміни можуть бути збільшені за письмовим дозволом декана.

Поведінка в аудиторії: На заняття студенти вчасно приходять до аудиторії відповідно до діючого розкладу та обов'язково мають дотримуватися вимог техніки безпеки.

Під час занять студенти:

- не вживають їжу та жувальну гумку;
- не залишають аудиторію без дозволу викладача;
- не заважають викладачу проводити заняття.

Під час контролю знань студенти:

- є підготовленими відповідно до вимог даного курсу;
- розраховують тільки на власні знання (не шукають інші джерела інформації або «допомоги» інших осіб);
- не заважають іншим;
- виконують усі вимоги викладачів щодо контролю знань.