Силабус курсу:

КІБЕРБЕЗПЕКА КРИТИЧНИХ ІНФРАСТРУКТУР

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Ступінь вищої освіти:	магістр
Спеціальність:	122 «Комп'ютерні науки», 123 «Комп'ютерна інженерія»
Рік підготовки:	1
Семестр викладання:	осінній
Кількість кредитів ЄКТС:	3
Мова(-и) викладання:	українська
Вид семестрового контролю	екзамен

Автор курсу та лектор:

к.т.н., доц., Кардашук Володимир Сергійович
вчений ступінь, вчене звання, прізвище, ім'я та по-батькові
доцент кафедри комп'ютерних наук та інженерії
посада

kardashuk@snu.edu.ua	+380954779243	Skype, Viber	405 НК, за розкладом
електронна адреса	телефон	месенджер	консультації

Викладач лабораторних занять:*

к.т.н., доц., Кардашук Володимир Сергійович
вчений ступінь, вчене звання, прізвище, ім'я та по-батькові
доцент кафедри комп'ютерних наук та інженерії
посада

kardashuk@snu.edu.ua	+380954779243	Skype, Viber	407НК, за розкладом
електронна адреса	телефон	месенджер	консультації

Викладач практичних занять:*

к.т.н., доц., Кардашук Володимир Сергійович
вчений ступінь, вчене звання, прізвище, ім'я та по-батькові
доцент кафедри комп'ютерних наук та інженерії
посада

kardashuk@snu.edu.ua	+380954779243	Skype, Viber	407НК, за розкладом
електронна адреса	телефон	месенджер	консультації

Анотація навчального курсу

Цілі вивчення курсу:	Наведені в курсі матеріали спрямовані на формування у студентів знань і навичок в питаннях щодо захисту сучасного стану кібербезпеки в Україні, законодавчої бази, що регулює питання кібербезпеки, захисту від кібератак на об'єкти критичної інфраструктури, процеси трансформації та удосконалення кіберзахисту. Розглянуті питання дозволяють одержати поглиблене уявлення про суть розглянутих процесів з питань кіберзахисту для самостійного освоєння матеріалу та подальшого практичного використання. В основу рішення практично важливих проблем кібербезпеки та роботи ключових інформаційних систем загального користування впливає багато факторів: кібератаки, порушення, викликані форс-мажорними обставинами, вихід з ладу програмного та апаратного забезпечення, людські помилки. Перераховані явища наочно демонструють, наскільки сучасне суспільство залежить від стабільності роботи інформаційних систем. Курс може бути корисним студентам за спеціальностями в галузі «12. Інформаційні технології», а також майбутнім спеціалістам, менеджерам, що планують працевлаштування на підприємства та фірми діяльність яких пов'язана з інформаційними технологіями та кібербезпекою.
Результати навчання:	Знати: основні теоретичні положення щодо забезпечення захисту інформаційних ресурсів від кіберзагроз та вірусних програм для зменшення впливу на них хакерских атак та інших негативних факторів, що впливають на безпеку даних . Вміти: застосовувати сучасну наукову теорією, програмно-технічні засоби й методологічні підходи для вирішення науково-практичних задач по захисту інформаційних ресурсів від шкідливих впливів.
Передумови до початку вивчення:	Базові знання з програмування, комп'ютерної схемотехніки, структури баз даних, діагностики комп'ютерних мереж.

Мета курсу (набуті компетентності)

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

1. Навички використання інформаційних і комунікаційних технологій.
2. Здатність генерувати нові ідеї (креативність).
3. Здатність поставити задачу і визначити шляхи вирішення проблеми програмними засобами, знання методів пошуку оптимального рішення за умов неповної інформації про загрози інформаційним ресурсам.
4. Здатність описати, класифікувати та змоделювати широке коло кібератак, порушення, викликані форс-мажорними обставинами, вихід з ладу програмного та апаратного забезпечення, людські помилки. Перераховані явища наочно демонструють, наскільки сучасне суспільство залежить від стабільності роботи інформаційних систем.

Структура курсу

№	Тема	Години (Л/ЛБ/ПЗ)	Стислий зміст	Інструменти і завдання
1.	Стан кібербезпеки в Україні	2/0/0	Сучасність та майбутнє кібербезпеки в Україні. Україна на кіберкарті Європи. Сучасні тренди кібербезпекової політики: висновки для України.	Участь в обговоренні Індивідуальні завдання
2.	Кібербезпека як важлива складова всієї системи захисту держави	2/4/0	Кібернетичні операції як невід'ємна частина гібридної війни. Наслідки кібератак.	Участь в обговоренні Індивідуальні завдання
3.	Тенденції розвитку кібербезпеки	4/0/0	Удосконалення розвитку кібератак. Збільшення рівня контролю за користувачами мережі Інтернет. Посилення регулювання на національному та міжнародному рівнях діяльності в кіберпросторі і зростання ролі приватного сектора .	Участь в обговоренні Індивідуальні завдання
4.	Заходи щодо реалізації концепції кібербезпеки	2/0/0	Об'єкти критичної інфраструктури. Складові кібербезпеки.	Участь в обговоренні Індивідуальні завдання
5.	Нові види діяльності кіберзлочинців і боротьба з ними	3/0/0	Зростання загроз для соціальних мереж та функціонування бізнесу. Кіберскладова сучасних конфліктів. Кіберскладова сьогодення. Стан і перспективи кібербезпекового сектора України.	Участь в обговоренні Індивідуальні завдання
6.	Кіберзахист провідних країн світу та ситуація із забезпеченням кібербезпеки в Україні	2/0/0	Резолюція ООН по створенню глобальної культури кібербезпеки. Процеси трансформації та удосконалення кіберзахисту. Ситуація із забезпеченням кібербезпеки в Україні.	Участь в обговоренні Індивідуальні завдання
7.	Стратегія кібербезпеки в Україні	2/0/0	Безпека в мережі: як Україна регулюватиме кіберпростір. Кібербезпека - проблема століття.	Участь в обговоренні Індивідуальні завдання
8.	Лабораторна робота № 1	0/4/0	Вивчення програм хешування для перевірки цілісності. Програма хешування може бути використана для перевірки - змінилися дані, чи вони залишилися незмінними. Програма хешування обчислює хеш-функцію з даних або файлу, та повертає значення (як правило, набагато коротше). Є багато різних хеш-функцій, деякі дуже прості, а деякі дуже складні. Коли однакова хеш-функція виконується з однаковими даними, то значення, що повертається, завжди однакове. Якщо з даними відбуваються будь-які зміни, то повернене значення хешу буде іншим.	Індивідуальні завдання

№	Тема	Години (Л/ЛБ/ПЗ)	Стислий зміст	Інструменти і завдання
9.	Лабораторна робота № 2	0/4/0	Створення та збереження надійних паролів. Паролі широко використовуються для захисту доступу до ресурсів. Зловмисники можуть використовувати багато методів для розкриття паролів користувачів та отримання несанкціонованого доступу до ресурсів або даних. Щоб краще захистити себе, важливо розуміти, що робить пароль надійним і як його безпечно зберігати.	Індивідуальні завдання
10.	Лабораторна робота № 3	0/4/0	Команди й основні інструменти операційної системи Windows. Команди мають вбудовані функції операційної системи. Інструменти роблять більше: досліджують мережі, шукають хости (англ. «host») (так називаються комп'ютери, підключені до мережі), і дозволяють побачити або встановити інформацію про маршрутизацію хосту.	Індивідуальні завдання
11.	Практична робота № 1	0/0/2	Дослідження утиліти netcat. Утиліта nc (або netcat). nc - програма для створення з'єднань з використанням сокетів протоколів TCP і UDP і подальшою передачею даних по ним. Вона дозволяє як здійснювати клієнтські підключення з використанням зазначених протоколів, так і створювати на серверній стороні сокети, що знаходяться в режимі очікування вхідних з'єднань від клієнтів.	Індивідуальні завдання
12.	Практична робота № 2	0/0/2	Службові програми - утиліти (ipconfig, ping, traceroute, netstat, telnet та ін.). В операційних системах Microsoft Windows ipconfig - це утиліта командного рядка для виводу деталей поточного з'єднання і управління клієнтськими сервісами DHCP і DNS. Також є подібні графічні утиліти: winipcfg і wntipcfg (остання передувала ipconfig). Утиліта ipconfig дозволяє визначати, які значення конфігурації були отримані за допомогою DHCP, APIPA або іншої служби IP-конфігурації або задані адміністратором вручну.	Індивідуальні завдання
13.	Практична робота № 3	0/0/2	Визначення затримки мережі за допомогою утиліт «ping» і «traceroute». Утиліта дозволяє виміряти і оцінити затримку мережі за певний час і скласти наочні приклади типової активності мережі	Індивідуальні завдання

14.	Практична робота № 4	0/0/2	Налаштування режиму тунелю VPN На практиці локальна мережа через VPN являє собою лінію зв'язку між комп'ютерами на основі звичайного з'єднання через Інтернет. При цьому неважливо, через які саме вузли Глобальної Мережі буде встановлено це з'єднання, але можна не сумніватися - трафік піде по захищеній мережі. Таке виділене VPN-з'єднання прийнято називати тунелем.	Індивідуальні завдання
15.	Практична робота № 5	0/0/2	Налаштування VPN через MicroTik розглянуто приклад побудови VPN-тунелю для підключення до домашньої мережі на базі маршрутизатора виробництва MikroTik.	Індивідуальні завдання
16.	Практична робота № 6	0/0/2	Підключення та налаштування комутатора. Комутатор — це на зразок мосту між комп’ютерами та мережею. На відміну від концентратора, такий пристрій здатний передавати пакети визначеному одержувачу, що знижує навантаження на мережу шляхом оптимізації її роботи. Це також позитивно позначається на безпеці.	Індивідуальні завдання
17.	Практична робота № 7	0/0/2	Програ́ми віддáленого доступу (адміністрування) — програми або функції операційних систем, що дозволяють отримати віддалений доступ до комп'ютера через Інтернет або локальну мережу і здійснювати управління та адміністрування віддаленого комп'ютера в реальному часі.	Індивідуальні завдання

Рекомендована література

1. Закон України «Про основні засади забезпечення кібербезпеки України» (Редакція від 08.07.2018) [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19

2. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України” [Електронний ресурс]. – Режим доступу: https://uacs.kiev.ua/resources-ua/legislative-framework-ua/cyber-strategy/

3. F-Secure: Человечество стоит на пороге развития гонки кибервооружения [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/428659.php

4. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015. – 288 с.

5. Безкоровайный М.М. Кибербезопасность – подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. – № 1(2). – 2014. – С. 22-27.

6. Поняття та зміст системи забезпечення кібербезпеки [Електронний ресурс]. – Режим доступу: http://goal-int.org

7. Настанови з кібербезпеки від експертів [Електронний ресурс]. – Режим доступу:http://www.isaca.org.ua/ index.php/press-center/news/191-translation-of-guidelines-on-cybersecurity

8. Мельник С. В. Актуальні напрями попередження правопорушень у кіберпросторі як складова стратегії кібернетичної безпеки держави Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ / С. В. Мельник, В. І. Кащук. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

9. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України. Аналітична доповідь. / Д.В. Дубов, М.А. Ожеван. – К.: НІСД, 2011. – 30 с.

10. Шеломенцев В. П. Формування законодавчих основ забезпечення кібербезпеки України / В. П. Шеломенцев // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

11. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 312–320.

12. Морозюк С. П. Шляхи підвищення рівня безпеки кібернетичного простору України / С. П. Морозюк // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

13. Бабич Є. Ю. Забезпечення кібербезпеки в Україні / Є. Ю. Бабич // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. – Кропивницький : КНТУ, 2016. – С. 77–78.

14. Єрьоміна Л. В. Напрями удосконалення законодавства України у сфері кібербезпеки: термінологічний аспект / Л. В. Єрьоміна // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

15. Цаль-Цалко Ю.С. Облікова політика підприємства та її кібербезпека / Ю.С. Цаль-Цалко, Ю.Ю. Мороз // Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства: збірник наукових праць, том IV, частина І, Житомир: ПП «Рута», 2017 – С. 8-11.

16. Сисоєв В. Аналіз рівня освіти та підготовки фахівців з управління ІТ та інформаційної безпеки в Україні. Режим доступу: http://www.auditagency.com.ua/blog/ISACA_researc h_ Education.pdf.

17. Бурячок В. Л. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки / В. Л. Бурячок, С. О. Гнатюк, О. Г. Корченко // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013.

Методичне забезпечення

1. Текст лекцій з дисципліни «Кібербезпека критичних інфраструктур» (для здобувачів другого ступеня вищої освіти спеціальності 122 «Комп'ютерні науки», 123 «Комп'ютерна інженерія») / Уклад.: В. С. Кардашук – Сєвєродонецьк: Вид–во СНУ ім. В. Даля, 2021. – 80 с.
2. Методичні вказівки до виконання лабораторних робіт з дисципліни «Кібербезпека критичних інфраструктур» (для здобувачів другого ступеня вищої освіти спеціальності 122 «Комп'ютерні науки», 123 «Комп'ютерна інженерія») / Уклад.: В. С. Кардашук – Сєвєродонецьк: Вид–во СНУ ім. В. Даля, 2021. – 18 с.
3. Методичні вказівки до виконання практичних робіт з дисципліни «Кібербезпека критичних інфраструктур» (для здобувачів другого ступеня вищої освіти спеціальності 122

«Комп'ютерні науки», 123 «Комп'ютерна інженерія») / Уклад.: В. С. Кардашук – Сєвєродонецьк: Вид–во СНУ ім. В. Даля, 2021. – 69 с.

Оцінювання курсу
Шкала оцінювання студентів

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
		для екзамену
90 – 100	A	відмінно
82-89	B	добре
74-81	C	
64-73	D	задовільно
60-63	E	
35-59	FX	незадовільно з можливістю повторного складання
0-34	F	незадовільно з обов’язковим повторним вивченням дисципліни

Політика курсу

Плагіат та академічна доброчесність:	Студент може пройти певні онлайн-курси, які пов'язані з темами дисципліни, на онлайн-платформах. При поданні документу про проходження курсу студенту можуть бути перезараховані певні теми курсу та нараховані бали за завдання. 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.