МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)

_____ М. В. Афанасьєв

БЕЗПЕКА В СОЦІАЛЬНИХ МЕРЕЖАХ

робоча програма навчальної дисципліни

Галузь знань	**усі галузі**
Спеціальність	**усі спеціальності**
Освітній рівень	**другий (магістерський)**
Освітня програма	**усі освітні програми**

Вид дисципліни	**вибіркова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри *Кібербезпеки та інформаційних технологій* Євсеєв С.П.

Харків
ХНЕУ ім. С. Кузнеця
2019

ЗАТВЕРДЖЕНО
на засіданні кафедри Кібербезпеки та інформаційних технологій
Протокол № 6 від 10.12.2019 р.

Розробники:
Євсеєв С.П., д.т.н., с.н.с., завідувач кафедри КІТ,
Король О.Г., к.т.н., доц. кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

1. Вступ

Програма вивчення навчальної дисципліни “Безпека в соціальних мережах” складена відповідно до освітньої програми підготовки магістрів зі всіх спеціальностей.

Анотація навчальної дисципліни: В еру високих технологій формування соціуму не можливо без використання сучасних технологій соціальних мереж в кіберпросторі. Важливою рисою їх використання є забезпечення безпеки не тільки персональних даних особистості, но її інформаційної безпеки держави. В сучасному кіберпросторі загрози набули ознак гібридності та синергізму, що дозволяє збільшувати рівень ризиків зламу технічних засобів забезпечення безпеки та несанкціонованого отримання конфіденційної інформації. Забезпечення безпеки персональних даних грамотне використання сучасних технічних (програмних) застосунків безпеки є невід’ємною частиною успішної особистості, має надати конкурентні переваги магістрам різних спеціальностей на ринку працевлаштування

Дисципліна “Безпека в соціальних мережах” є навчальною дисципліною вільного вибору (вільний магмайнор) за усіма спеціальностями. Вона викладається у другому семестрі магістратури в обсязі 150 год.(5 кредитів ECTS), зокрема: лекції – 20 год., лабораторні – 20 год., самостійна робота – 110 год, консультації – 4 год. У курсі передбачено два змістових модулі та дві модульні контрольні роботи. Завершується дисципліна заліком.

Об’єктом навчальної дисципліни є технології кіберпростору, соціальних мереж, механізми забезпечення послуг безпеки.

Предметом навчальної дисципліни є правові та практичні основи використання, принципи функціонування та забезпечення безпеки персональних даних (конфіденційної інформації) в соціальних мережах.

Мета навчальної дисципліни:

є засвоєння принципів забезпечення безпеки персональних даних (конфіденційної інформації) в соціальних мережах, використання механізмів послуг безпеки в умовах сучасних загроз.

Основними завданнями вивчення навчальної дисципліни є:

ознайомлення з правовими аспектами забезпечення інформаційної і кібербезпеки на рівні держави, міжнародному рівні;

ознайомлення з принципами побудови соціальних мереж, протоколами обміну даними в кіберпросторі;

ознайомлення з сучасними програмними (програмно-апаратними) застосунками забезпечення безпеки персональних даних;

навчитися орієнтуватися в сучасних загрозах, їх направленості;

навчитися аналізувати ризики використання конфіденційної інформації в соціальних мережах, відрізняти фейкову інформацію в медіапросторі;

навчитися орієнтуватися у послугах і механізмах забезпечення безпеки;

набути практичних здатностей в забезпеченні безпеки особистих персональних даних в умовах сучасних загроз.

Курс	**1**	
Семестр	**1**	
Кількість кредитів ECTS	**5**	
Аудиторні навчальні заняття	**лекції**	**20**
	лабораторні	**20**
Самостійна робота		**110**
Форма підсумкового контролю	**Залік диференційований**	

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
Здатність забезпечити захист персональних даних (конфіденційної інформації) в кіберпросторі	вміти обирати найбільш зручні механізми забезпечення основних послуг безпеки; вміти аналізувати сучасний стан гібридних загроз; вміти використовувати криптографічні застосунки, розуміти їх вимоги та ризики їх використання.
Здатність розв'язувати практичні задачі у галузі забезпечення інформаційної та\або кібербезпеки під час виконання службових обов'язків.	знати основні кіберзагрози в сучасних комп'ютерних, соціальних мережах, способи тестування програмних застосунків механізмів захисту; вміти виявляти загрози/уразливості, що загрожують безпеці в соціальних (комп'ютерних) мережах, формувати пропозиції щодо використання криптографічних алгоритмів для забезпечення безпеки персональних даних (конфіденційної інформації) в Інтернет-технологіях

3. Програма навчальної дисципліни

Змістовий модуль 1. Безпека і захист даних

Тема 1. **Огляд безпеки системи**

Основні поняття та визначення безпеки. Роль захисту інформації в кіберпросторі, умови функціонування підсистеми безпеки в соціальних (комп'ютерних) мережах та системах. Вимоги щодо безпеки системи, ризики безпеки. Складові та послуги безпеки: конфіденційність, цілісність, доступність, причетність, спостережність. Розподіл послуг безпеки за рівнями моделі ISO/OSI. Критерії захищеності комп'ютерних систем. Національні нормативні акти і міжнародні регулятори системи безпеки

Тема 2. **Сучасні загрози в соціальних (комп'ютерних) мережах**

Формальне визначення криптосистеми. Критерії та показники ефективності. Аналіз основних видів атак, ризиків та вразливих на елементи інформаційних систем в кіберпросторі. Синергія та гібридність сучасних загроз, основні тенденції спрямованості.

Тема 3. **Механізми забезпечення конфіденційності та цілісності.**

Принципи побудови симетричного та несиметричного шифрування. Основні критерії їх використання. Блочні симетричні шифри, алгоритми блокового симетричного шифрування DES, ГОСТ-28147, Rijndael, Калина-256. Несиметричні криптосистеми RSA, Ель Гамаля та Діффі – Геллмана. Принципи їх використання с соціальних мережах.

Тема 4. **Механізми забезпечення автентичності**

Класифікація механізмів автентифікації: MDC-коди, MAC-коди, цифровий підпис. Основні стандарти цифрового підпису. Класифікація механізмів автентифікації на основі методів двофакторній автентифікації. Класифікація загроз на процедури двофакторній автентифікації. Основні вимоги до протоколів двофакторній автентифі-

кації. Основні процедури, які забезпечують безпеку в протоколах двофакторній автентифікації.

Тема 5. **Основи цифровій стеганографії**

Класифікація методів цифровій стеганографії з відкритим ключем. Основні методи приховування конфіденційної інформації.

Змістовий модуль 2. Мережева безпека

Тема 6. **Протоколи захисту інформації на мережевому рівні**

Захист інформації на мережному рівні. Протоколи захисту та цілісності IPSec, SSL, TLS, їх сутність. Системи захисту PGP та CS MIME. Криптографічні функції. Сумісність на рівні електронної пошти. Захищена електронна пошта

Тема 7. **Механізми та протоколи керування ключами в ІВК в соціальних мережах**

Компоненти та сервіси інфраструктури відкритих ключів. Архітектура і топологія PKI. Основні вимоги стандарту відкритих ключів, управління сертифікатами. Системи PKI. Основні вимоги до політиці PKI.

Тема 8. **Програмно-апаратні засоби захисту інформації в мережі Internet**

Основні принципи захисту інформації при підключенні до мережі Інтернет. Використання паролів і механізмів контролю.

Тема 9. **Програмно-апаратні (програмні) засоби захисту інформації в мережі Wi-Fi**

Основні принципи захисту інформації при підключенні до мережі Wi-Fi. Використання паролів і механізмів контролю. Основні вимоги стандарту безпеки технології DTE (4G).

Тема 10. **Програмно-апаратні (програмні) засоби захисту інформації в хмарних технологіях**

Основні принципи захисту інформації при використанні хмарних мереж (технологій).

Теми лабораторних занять:

1. Механізми захисту операційної системи Windows 10.
2 Вивчення можливостей захисту шифрованої файлової системи (EFS) Windows 10, центру безпеки та обслуговування і брандмауера Windows 10.
3. Засоби автентифікації користувачів і аналізу безпеки системи
4. Засоби аналізу захищеності.
5. Дослідження стійкості парольного захисту.

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, семінарські, практичні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця, контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних і лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

модульний контроль, що проводиться у формі контрольної роботи за відповідний змістовий модуль;

підсумковий/семестровий контроль, що проводиться у формі заліку, відповідно

до графіку навчального процесу.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час лекційних і лабораторних занять та виконання індивідуальних завдань проводиться за такими критеріями:

здатність забезпечити захист персональних даних (конфіденційної інформації) в кіберпросторі;

здатність розв'язувати практичні задачі у галузі забезпечення інформаційної та\або кібербезпеки під час виконання службових обов'язків.

Результатами навчання є: вміння обирати найбільш зручні механізми забезпечення основних послуг безпеки, аналізувати сучасний стан гібридних загроз. Знання основних кіберзагроз в сучасних комп'ютерних, соціальних мережах, способів тестування програмних застосунків механізмів захисту. Вміння виявляти загрози/уразливості, що загрожують безпеці в соціальних (комп'ютерних) мережах, формувати пропозиції щодо використання криптографічних алгоритмів для забезпечення безпеки персональних даних (конфіденційної інформації) в Інтернет-технологіях, та використовувати криптографічні застосунки, розуміти їх вимоги та ризики їх використання.

Загальними критеріями, за якими здійснюється оцінювання позааудиторної самостійної роботи студентів, є: глибина і міцність знань, рівень мислення, вміння систематизувати знання за окремими темами, вміння робити обґрунтовані висновки, володіння категорійним апаратом, навички і прийоми виконання практичних завдань, вміння знаходити необхідну інформацію, здійснювати її систематизацію та обробку, самореалізація на практичних та семінарських заняттях.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі заліку, який вважається зданим успішно, якщо студент упродовж семестру набрав 60 і більше балів.

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – "зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Розподіл балів за тижнями

Теми змістового модуля			Лекційні заняття	Лабораторні заняття	Захист лабораторних занять	Експрес-опитування	Письмова контрольна робота	Усього
Змістовний модуль	Тема	Тиждень						
Змістовий модуль 1	1	1	1					1
	2	2	1	1	4	3		9
	3	3	1					1
		4		1	4	3		8
	4	5	1					1
		6		1	4	3		8
	5	7	1	1		3		5
		8		1		3	11	15

Теми змістового модуля			Лекційні заняття	Лабораторні заняття	Захист лабораторних занять	Експрес-опитування	Письмова контрольна робота	Усього
Змістовний модуль	Тема	Тиждень						
Змістовий модуль 2	6	9	1		4			5
	7	10	1	1		3		5
		11		1	4	3		8
	8	12	1	1		3		5
		13		1	4	3		8
	9	14	1	1		3		5
		15		1	4		11	16
	10	16	1					1
	Залік							
Усього			10	10	28	30		100

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	Зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

5. Рекомендована література

5.1 Основна.

1. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ- 2000”, 2019. – 678.

2. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С. Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6

3. Грищук Р. В., Даник Ю. Г. Основы кибербезопасности: монография / отв. ред. проф. Ю. Г. Даник, Житомир : ЖНАЕУ, 636 с., 2016.

4. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.: ил. – Парал. тит. англ.

5. Олифер В, Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – СПб.: Питер, 2016. – 992 с.

5.2. Додаткова

6. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.

7. Хорошко В. А. Методы и средства зашиты информации. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с

5.3. Інформаційні ресурси в Інтернеті

8. https://pns.hneu.edu.ua/course/view.php?id=5626