МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Кафедра захисту інформації

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРОТОКОЛИ ЦИФРОВОГО ПІДПИСУ

Освітня програма: Безпека інформаційних і комунікаційних систем

Спеціальність: 125 Кібербезпека

Галузь знань: 12 Інформаційні технології

Ступінь вищої освіти: Перший (бакалаврський) рівень

Затверджено на засіданні кафедри
захисту інформації
Протокол №____ від _____ р.

м. Запоріжжя 2020

1. Загальна інформація	
Назва дисципліни	*ППВС 04. Протоколи цифрового підпису, вибіркова частина. цикл дисциплін вільного вибору студента.*
Рівень вищої освіти	*Перший (бакалаврський) рівень*
Викладач	*Козіна Галина Леонідівна, к.ф.-м.н., доцент.*
Контактна інформація викладача	*Телефон кафедри 7698491, викладача 7698597, kozina@zp.edu.ua*
Час і місце проведення навчальної дисципліни	*Згідно розкладу занять викладачів кафедри.* https://zp.edu.ua/kafedra-zahistu-informaciyi
Обсяг дисципліни	*3 кредита ЄКТС, 90 годин.* *Розподіл годин:* *40 годин теоретичні та практичні заняття: лекції 20 годин, лабораторні 20 годин; самостійна робота 50 годин.* *Семестр вивчення навчальної дисципліни: 8 семестр.* *Вид контролю: залік в кінці 8 семестру.*
Консультації	*Згідно з графіком консультацій.* https://zp.edu.ua/kafedra-zahistu-informaciyi

2. Пререквізіти і постреквізіти навчальної дисципліни

Пререквізіти: Основи криптографії та стеганографії (теми: електронний цифровий підпис, функція хешування, аналіз складності).
Компетентності:
КЗ 1. Здатність застосовувати знання в практичних ситуаціях.
КЗ 8. Здатність використовувати знання базових розділів фізики і математики в обсязі, необхідному для засвоєння фахових дисциплін.
Постреквізіти: Проектування, впровадження та супровід комплексних систем захисту інформації

3. Характеристика навчальної дисципліни

Дисципліна «Протоколи цифрового підпису» є вибірковою у підготовці фахівця з інформаційної безпеки.

Перелік загальних и фахових компетентностей, яких набуває студент при вивченні:
КЗ 1. Здатність застосовувати знання в практичних ситуаціях.
КЗ 4. Вміти виявляти, ставити та вирішувати проблеми за професійним спрямуванням, здійснювати професійну діяльність на основі техніко-економічного аналізу.
КЗ 8. Здатність використовувати знання базових розділів фізики і математики в обсязі, необхідному для засвоєння фахових дисциплін.
КФ 3. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.
КФ 6. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах, з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
КФ 11. Здатність застосовувати методи та засоби криптографічного, стеганографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

Програмні результати навчання:
ПРН 8. Використовувати знання про фізичні явища та володіти математичним апаратом для моделювання об'єктів інформаційної діяльності
ПРН 9. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки
ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН 31 Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного та стеганографічного захисту інформації.

4. Мета вивчення навчальної дисципліни

Формування у студентів здатності здійснювати практичне використання сучасних протоколів цифрового підпису в системах захисту інформації.

5. Завдання вивчення дисципліни

Основне завдання навчальної дисципліни – формування у студентів системних знань і компетентностей зі знання протоколів цифрового підпису різного призначення, базових алгоритмів криптографічних перетворень на еліптичних кривих для застосування в інформаційних і телекомунікаційних системах.

6. Зміст навчальної дисципліни

Змістовий модуль 1.

Тема 1. Колективний підпис.

Тема 2. Композиційний підпис.

Тема 3. Спарювання Вейля точок еліптичної кривої.

Тема 4. Кільцевий підпис.

Змістовий модуль 2.

Тема 5. Німецький стандарт підпису EC-GDSA.

Тема 6. Корейський стандарт підпису EC-KCDSA.

Тема 7. Сліпий підпис на базі алгоритму ЕльГамаля.

Тема 8. Анонімність схеми сліпого підпису.

Тема 9. Протокол сліпого підпису на базі німецького стандарту EC-GDSA.

Тема 10. Перевірка на анонімність сліпого підпису на базі німецького стандарту EC-GDSA.

7. План вивчення навчальної дисципліни

№ тижня	**Назва теми Форми організації навчання**		**Кількість годин**
1	*Колективний підпис*	лк	2
	Лабораторна робота №1. Протокол колективного підпису	лб	2
2	*Композиційний підпис*	лк	2
	Лабораторна робота №2. Протокол композиційного підпису.	лб	2
3	*Спарювання Вейля точок еліптичної кривої Кільцевий підпис*	лк	4
	Лабораторна робота №3. Протокол кільцевого підпису	лб	4
Рубіжний контроль.			
4	*Німецький стандарт підпису EC-GDSA*	лк	2
	Лабораторна робота №4. Німецький стандарт підпису EC-GDSA	лб	2
5	*Корейський стандарт підпису EC-KCDSA.*	лк	2
	Лабораторна робота №5. Корейський стандарт підпису EC-KCDSA	лб	2
6	*Сліпий підпис.*	лк	2
	Лабораторна робота №6. Протокол сліпого підпису на базі алгоритму цифрового підпису ЕльГамаля.	лб	2
7	*Анонімність схеми сліпого підпису.*	лк	2
	Лабораторна робота №7. Дослідження анонімності в протоколі сліпого підпису на базі алгоритму цифрового підпису ЕльГамаля.	лб	2
8	*Протокол сліпого підпису на базі німецького стандарту EC-GDSA*	лк	2
	Лабораторна робота №8. Протокол сліпого підпису на базі німецького стандарту EC-	лб	2

	GDSA		
9	*Перевірка на анонімність сліпого підпису на базі німецького стандарту EC-GDSA.*	лк	2
	Лабораторна робота №9. Дослідження анонімності в протоколі сліпого підпису на базі німецького стандарту EC-GDSA	лб	2
Рубіжний контроль. Підсумковий семестровий контроль - залік.			

8. Самостійна робота

Самостійна робота включає в себе: вивчення теоретичного матеріалу, підготовку до лабораторних робіт, підготовку до рубіжного та підсумкового контролю.

№ тижня	Назва теми	Кількість годин	Консультації, годин
1-2	*Колективний підпис. Композиційний підпис.*	*4*	*0,1*
	Підготовка до лабораторних занять.	*4*	*0,1*
3-5	*Спарювання Вейля точок еліптичної кривої. Кільцевий підпис*	*4*	*0,1*
	Підготовка до лабораторних занять	*4*	*0,1*
Підготовка до рубіжного контролю. Рубіжний контроль.		*4*	*0,4*
6-7	*Німецький стандарт підпису EC-GDSA. Корейський стандарт підпису EC-KCDSA*	*4*	*0,1*
	Підготовка до лабораторних занять.	*4*	*0,1*
8-9	*Сліпий підпис. Анонімність схеми сліпого підпису на базі алгоритму цифрового підпису ЕльГамаля.*	*4*	*0,1*
	Підготовка до лабораторних занять.	*4*	*0,1*
10	*Протокол сліпого підпису на базі німецького стандарту EC-GDSA. Перевірка на анонімність сліпого підпису на базі німецького стандарту EC-GDSA.*	*4*	*0,1*
	Підготовка до лабораторних занять.	*4*	*0,1*
Підготовка до рубіжного контролюю. Рубіжний контроль.		*6*	*0,4*
Підсумковий семестровий контроль - залік.		*2*	*0,2*

9. Система та критерії оцінювання курсу

Поточний, рубіжний, семестровий контроль (з урахуванням відвідування занять, виконання лабораторних робіт, тестування при здачі модулів та заліку).

Форма проведення контролю: усна, письмова, комбінована, а також шляхом тестування з використанням програмно-технічних засобів.

9.1 Розподіл балів, які отримують студенти

Рубіжний контроль					
Змістовий модуль №1			*Змістовий модуль № 2*		
Тема 1-Тема 4	*Лабораторна робота №1-№3*	*Сума 1*	*Тема 5-Тема 10*	*Лабораторна робота №4-№9*	*Сума 2*
40	*60*	*100*	*40*	*60*	*100*

Підсумковий семестровий контроль					
Бали за змістові модулі	*Сума*	*Бали за семестровий контроль*	*Сума*	*Залік*	*Сума*
0.4 (Сума 1+ Сума 2)	*80*		*20*		*100*

9.2 Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	*Оцінка ECTS*	*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 з можливістю повторного складання*	*не зараховано з можливістю повторного складання*
0-34	***F***	*незадовільно з обов'язковим повторним вивченням дисципліни*	*не зараховано з обов'язковим повторним вивченням дисципліни*

10. Політика курсу

Викладач пояснює студентам систему організації навчального процесу та правил поведінки студентів на заняттях. Усі завдання, передбачені програмою, мають бути виконані у встановлені терміни. Успішність засвоєння навчального матеріалу визначається числом балів, отриманих при контрольних заходах. Максимальне число балів за змістовий модуль дорівнює 100: 40 балів за результатами тестування з теоретичного матеріалу, 60 балів за виконання лабораторних робіт. Кожна лабораторна робота оцінюється 12-20 балами: приблизно 5 балів за відповіді на контрольні питання до роботи, 10 балів за виконання і захист роботи. Максимальне число балів підсумкового семестрового контролю дорівнює 100 і складаються: з суми балів змістових модулів, помноженої на коефіцієнт 0,4 - разом 80 балів, і додаткових 20 балів при опитуванні під час заліку. Студенти, які отримали при змістовому модульному контролі менше 60 балів до підсумкового семестрового контролю не допускаються.

Під час навчання студенти зобов'язані дотримуватися академічної доброчесності:

- самостійно виконувати навчальні завдання, завдання поточного та підсумкового контролю;
- дотримуватися норм законодавства про авторське право;
- приймати активну участь у навчальному процесі;
- не запізнюватися на заняття, не пропускати заняття без поважних причин;
- самостійно і своєчасно вивчити матеріал пропущеного заняття;
- давати достовірну інформацію про результати власної навчальної діяльності.
- бути терпимим і доброзичливим до однокурсників та викладачів.

Інформаційні ресурси:

https://zp.edu.ua
http://library.zp.edu.ua:8081/lib2web/DocSearchForm
http://e-library.zp.edu.ua
https://zp.edu.ua/kafedra-zahistu-informaciyi