МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Східноєвропейський національний університет імені Лесі Українки
Кафедра національної безпеки

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної і
навчальної роботи та рекрутації
проф. Гаврилюк С. В. _____
Протокол № 2 від «16» жовтня 2019 р.

№8216102019

ПРОГРАМА
нормативної навчальної дисципліни

Основи криптографічного захисту
підготовки бакалавра

галузі знань: 12 Інформаційні технології
спеціальності 125 Кібербезпека
освітньо-професійної програми (спеціалізації)Інформаційна безпека

Луцьк – 2019

Програма навчальної дисципліни“ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ**”** підготовки бакалавра, галузі знань 12 “Інформаційні технології”, спеціальності 125 “Кібербезпека”,за освітньо-професійною програмою (спеціалізацією) “Інформаційна безпека”.

Розробник: Глинчук Л. Я., кандидат фізико-математичних наук, старший викладач кафедри національної безпеки.

Рецензент: Кузьмич О. І., кандидат фізико-математичних наук, доцент кафедри комп’ютерної інженерії та кібербезпеки ЛНТУ

Рецензент: Булатецька Л. В., кандидат фізико-математичних наук, доцент кафедри прикладної математики та інформатики СНУ ім. Лесі Українки

Програма навчальної дисципліни затверджена на засіданні кафедри національної безпеки

протокол № ___ від _____ 2019 р.

Завідувач кафедри: _____(М. А. Наход)

Програма навчальної дисципліни схвалена науково-методичною комісією факультету історії, політології та національної безпеки

протокол № ____від _____ 2019 р.

Голова науково-методичної
комісії факультету _____(А. Г. Шваб)

Програма навчальної дисципліни схвалена науково-методичною радою Східноєвропейського національного університету імені Лесі Українки

1.ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітня програма, освітній ступінь</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="8">Галузь знань: 12 “Інформаційні технології” спеціальність 125 “Кібербезпека” освітньо-професійна програма (спеціалізація) “Інформаційна безпека” Освітній ступінь: бакалавр</td><td>Нормативна</td></tr>
<tr><td>Рік навчання – 4</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 120/4</td><td>Семестр – 7</td></tr>
<tr><td>Лекції 20 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Практичні (семінарські) 22 год.</td></tr>
<tr><td>Самостійна робота 70 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td>Форма контролю: екзамен</td></tr>
</table>

2. АНОТАЦІЯ КУРСУ:

Дисципліна “ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ” належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра. Спрямована на вивчення симетричних та асиметричних методів шифрування інформації, їх використання; видів криптоаналізу та можливість його застосування.

Мета навчальної дисципліни: полягає вознайомленні із загальними поняттями та історією розвитку криптології; із симетричними та асиметричними методами шифрування; з основними напрямками використання криптографічних методів; з основними поняттями криптовалюти та її поширення у світі; з основами криптоаналізу; формування у студентів знань та умінь, які створять теоретичний і практичний фундамент, необхідний для аналізу необхідності застосування того чи іншого методу шифрування, а також можливість виконувати простий криптоаналіз.

Програмні результати навчання:

Бакалавр повинен знати: класичні криптографічні алгоритми – симетричні та асиметричні; напрями та сфери використання та застосування криптографічних алгоритмів; поняття криптовалюти та її поширення у світі; розрізняти основні види криптоаналізу і розуміти можливість його проведення; володіти методами захисту інформації в Інтернет-ресурсах;основи комп’ютерних мереж, володіти технологіями побудови та адміністрування мереж; володіти технологіями та методами

розроблення програмного забезпечення для захисту інформації в комп'ютеризованих системах та мережах.

*Бакалавр повинен вміти:*застосовувати алгоритми та методи захисту інформації у проектах комп'ютеризованих систем; застосовувати алгоритми криптографічного захисту; застосовувати методи криптоаналізу; контролювати та здійснювати моніторинг працездатності системного та прикладного програмного забезпечення в умовах експлуатації комп'ютеризованих систем; вміти контролювати та перевіряти правильність експлуатації встановленого програмного забезпечення комп'ютеризованої системи згідно чинних норм та стандартів.

3. КОМПЕТЕНЦІЇ

Загальні компетенції:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

Фахові компетенції:

КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.

КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та

інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

4. ІНФОРМАЦІЙНИЙ ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Програма навчальної дисципліни складається з таких **змістових модулів**:

1. Симетричні алгоритми шифрування.
2. Асиметричні алгоритми шифрування та основи криптоаналізу.

Структура навчальної дисципліни представляється у вигляді таблиці 2.

Таблиця 2

Назви змістових модулів і тем	**Кількість годин**						
	Усього	**у тому числі**					
		Лек.	**Практ.**	**Лаб.**	**Інд.**	**Сам. роб.**	**Конс.**
1	2	3	4	5	6	7	8
Змістовий модуль 1. Симетричні алгоритми шифрування							
Тема 1. Криптологія: основні поняття та історичний розвиток	10	2	2			6	
Тема 2. Класичні шифри перестановки	10	2	2			6	
Тема 3. Класичні шифри заміни	10	2	2			6	
Тема 4. Шифри, які використовують аналітичні перетворення	12	2	2			6	2
Тема 5. Шифри з використанням гамування	10	2	2			6	
Тема 6. Стандарт шифрування DES, GOST	18	2	4			10	2
Разом за модулем 1	70	12	14			40	4
Змістовий модуль 2. Асиметричні алгоритми шифрування та основи криптоаналізу							
Тема 7.Основні поняття асиметричної криптографії. Алгоритм RSA, система Діффі-Хелмана та Ель-Гамаля	14	2	2			8	2
Тема 8. Хеш-функція. Приклади хеш-функцій	12	2	2			8	
Тема 9. Загальні поняття криптоаналізу.	14	2	2			8	2

Дешифрування класичних шифрів							
Тема 10. Загальне поняття про криптовалюти. Передумови виникнення та поширення в Україні та в світі	10	2	2			6	
Разом за модулем 2	50	8	8			30	4
Всього годин:	120	20	22			70	8

5. ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

№ з/п	Тема	Кількість годин
1	Підготовка лабораторних робіт	**50**
2	Опрацювання лекцій	**20**
Разом		**70**

6. РОЗПОДІЛ БАЛІВ ТА КРИТЕРІЇ ОЦІНЮВАННЯ

Поточний контроль (max = 40 балів)										**Модульний контроль (max = 60 балів)**		**Загальна кількість балів**
Модуль 1										**Модуль 2**		
Змістовий модуль 1						**Змістовий модуль 2**				**МКР 1**	**МКР 2**	
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	20	40	100
4	4	4	4	4	4	4	4	4	4			

Шкала оцінювання (національна та ECTS)

Сума балів за всі види навчальної діяльності	**Оцінка ECTS**	**Оцінка за національною шкалою**	
		для екзамену, курсової роботи (проекту), практики	**для заліку**
90 – 100	A	Відмінно	Зараховано

82 – 89	B	Добре	
75 – 81	C		
67 -74	D	Задовільно	
60 – 66	E		
1 – 59	Fx	Незадовільно	Незараховано (з можливістю повторного складання)

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна література

1. Алгоритм обчислення хеш-функції MD5: Методичні вказівки до лабораторної роботи з курсу “Проектування засобів захисту інформації” для студентів напрямків 7.091501, 8.091501 “Комп’ютерні системи та мережі”, 8.091502 “Системне програмне забезпечення”, 8.091503 “Спеціалізовані комп’ютерні системи” / Укладачі: В.М. Грига, В.М. Сокіл – Львів: Національний університет “Львівська політехніка”, 2006, 11 с.
2. Баричев С.Г., Серов Р.Е. Основы современной криптографии. – М.: “Горячая линия – Телеком”, 2001. – 198 с.
3. Введение в криптографию / Под общ. ред. В.В. Ященко. – СПб.: Питер, 2001. – 288 с.: ил.
4. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Людмила Ярославівна Глинчук. – Луцьк: Вежа-Друк, 2014. – 164 с.
5. Грездов Г.Г. Современные методы криптографической защиты информации (Обзор по материалам открытой печати). – Киев. 2002.– 38 с.
6. Захарченко М.В., Йона Л.Г., Щербина Ю.В., Онацький О.В. Розвинення криптології та її місце в сучасному суспільстві: Навч. посібник. – Одеса: ОНАЗ ім. О.С. Попова, 2003. – 80 с.
7. Медведев М.Г. Ймовірнісні тести на простоту
8. Монастриський Л. С. Методичні вказівки до виконання лабораторних робіт з розділу комп’ютерна криптологія з курсу “Системи і методи захисту інформації” для студентів університету природничих спеціальностей. – Львів: Видавничий центр ЛНУ ім. Івана Франка, 2003. – 42 с.
9. Моргун О.М. Кріптографічні методи захисту інформації: Навч. посібник. – Черкаси: АПБ ім. Героїв Чорнобиля, 2008. – 97с.
10. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с., ил.

11. Саломаа А. Криптография с открытым ключом: Пер. с англ. – М.: Мир, 1995. – 318 с.
12. Смарт Н. Криптография. – М.: Техносфера, 2005, – 528 с.
13. Фомичев В.М. Дискретная математика и криптология. Курс лекций/ Под общ. ред. д-ра физ.-мат. н. Н.Д. Подуфалова. – М.: Диалог-Мифи, 2003. – 400 с.
14. Шнайер Б. Прикладная криптография, 2-е издание, Протоколы, алгоритмы и исходные тексты на языке С. – М.: "Триумф", 2001. – 610 с.

Додаткова література (інтернет-джерела)

1. Основы криптографии. Часть 1. [Електронний ресурс]. – Режим доступу до ресурсу:https://www.youtube.com/watch?v=t7kNtZ94u-Y&list=PL_8BBd8_xXlaRxaF8cianF8K4-zpd6mjG&index=2
2. Основы криптографии. Часть 2. [Електронний ресурс]. – Режим доступу до ресурсу:https://www.youtube.com/watch?v=mlMcNWTwxMw&list=PL_8BBd8_xXlaRxaF8cianF8K4-zpd6mjG&index=1
3. Классическая Криптография. [Електронний ресурс]. – Режим доступу до ресурсу:https://www.youtube.com/playlist?list=PLbnf75Jro21rz_PuugcnX3O3HYPfBPdc8

8. ПЕРЕЛІК ПИТАНЬ ДО ЕКЗАМЕНУ

1. Історичний розвиток криптології.
2. Можливість прихованої передачі інформації.
3. Основні поняття стеганографії.
4. Основні принципи криптології.
5. Поняття абсолютно стійкого шифру.
6. Основні поняття "криптографія", "криптологія", "криптоаналіз", "шифрування", "зламування шифру", "противник", "ключ", "симетричні методи шифрування", "асиметричні методи шифрування" та ін.
7. Класифікація шифрів за методом шифрування.
8. Класифікація шифрів за технологією шифрування.
9. Класифікація шифрів за особливостями ключів.
10. Основні характеристики сучасних методів шифрування.
11. Загальна характеристика класичних шифрів перестановки.
12. Загальна характеристика класичних шифрів заміни.
13. Класичні шифри перестановки.
14. Класичні шифри заміни.
15. Шифри, що використовують аналітичні перетворення.

16. Шифри з використанням гамування.
17. Стандарт шифрування даних DES.
18. Стандарт шифрування даних GOST.
19. Основні поняття асиметричних криптосистем.
20. Алгоритм RSA – криптографічна система з відкритим ключем.
21. Застосування алгоритму RSA.
22. Асиметричні криптосистеми – система Діффі-Хеллмана та Ель – Гамаля.
23. Односторонні функції і функції з лазівками.
24. Загальні поняття хеш-функцій.
25. Вимоги до хеш-функцій.
26. Криптографічні хеш-функції та поділ хеш-функцій.
27. Застосування хеш-функцій та способи їх злому.
28. Генератори псевдовипадкових чисел.
29. Основні ідеї хеш-функцій MD2, MD4, MD5 та MD6.
30. Алгоритм обчислення хеш-функції MD5.
31. Алгоритм обчислення хеш-функції SHA.
32. Загальні поняття криптоаналізу. Загальна класифікація різних типів криптоаналізу.
33. Загальні методи криптоаналізу для всіх типів криптографічних систем.
34. Популярні методи криптоаналізу.
35. Дешифрування класичних шифрів.
36. Методи криптоаналізу для симетричних криптосистем.
37. Дешифрування шифру простої заміни.
38. Дешифрування простої перестановки.
39. Поняття про криптовалюти. Історія їх виникнення.
40. Найбільш популярні криптовалюти.
41. Перспективи поширення криптовалют.