СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КРИПТОЛОГІЯ

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	125 Кібербезпека та захист інформації
Назва освітньо-професійної програми	Кібербезпека та захист інформації
Рівень вищої освіти	Другого (магістерського) рівня
Факультет	Інформаційни технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	**ОК-8** ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Басов Віктор Євгенович
basvic@bigmir.net

Старший викладач кафедри «Кібербезпеки та технічного захисту інформації»
Кандидат технічних наук за фахом 05.12.02 – Телекомунікаційні системи та мережі

Голєв Денис Володимирович
denis.veteran@gmail.com

Старший викладач кафедри «Кібербезпеки та технічного захисту інформації»

Загальна інформація про дисципліну

Анотація до дисципліни	Дисципліна «Криптологія»об’єднує та узагальнює такі дисципліни, як криптографія, криптоаналіз. Вона інтегрує, відповідно до свого предмету, знання з таких освітніх і наукових галузей: дискретна математика, теорія ймовірностей та комбінаторика, теорія зв’язку, теорія інформації, кодування. Навчання спрямовано на:

	1) формування у здобувачів вищої освіти системного уявлення про застосування та розробку криптографічних систем захисту інформації в процесах створення, зберігання та передавання конiфденційної інформації, а також чинників, що впливають на цей процес; 2) розвиток умінь з правильної експлуатації криптографічних систем, аналізу та розробки криптографічних протоколів, навичок оцінювання стійкості криптосистем до криптоаналітичних атак, та атак на криптографічні протоколи; 3) надання базових знань та первинних навичок до криптоаналізу як історичних, так і сучасних криптосистем та криптогафічніх протоколів; 4) аналіз та розробка криптографікних протоколів для розподілу ключів в секретних мережах зв'язку та протоколів розділення секрету.
Мета дисципліни	– формування системних знань та розвиток умінь щодо експлуатації, аналізу та розробки криптографічних систем захисту інформації при її створенні, зберіганні та передеванні через не захищене середовище..
Компетентності, формуванню яких сприяє дисципліна	КІ-1 Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність проводити дослідження на відповідному рівні. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу. КФ3 Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ8 Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
Результати навчання	РН1 Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2 Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3 Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4 Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5 Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

	РН6 Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7 Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН13 Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН21 Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН23 Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
Обсяг дисципліни	Загальний обсяг дисципліни: 4 кредитів ЄКТС 120 годин). Для денної форми навчання: лекції – 16 годин, практичні заняття –8 години, лабораторні заняття – 8 годин, самостійна робота – 86 годин.
Форма підсумкового контролю	Екзамен – 2 години
Терміни викладання дисципліни	Дисципліна викладається у 1-му семестрі (1–12 тижні)

Програма дисципліни

Тема 1.	***Технологія розрахунків над еліптичними кривими в полях Галуа.*** Алгебраїчні розрахунки над еліптичними кривими. Повна та скорочена форма Вєйєрштрасса запису рівняння еліптичної кривої. Будьяка пряма перетинає еліптичну криву у трьох крапках. Поняття нескінченно віддаленої крапки. Сума рьох крапок кривої, що належать одній перетинаючий прямій. Чому дорівнює сума двох крапок Додавання та подвоєння крапки. Дискретна еліптична крива в полі Галуа. Особливі та неособливі дискретні еліптичні криві
Тема 2.	***Двоключові криптосистеми над еліптичною кривою.*** Двоключовий алгоритм створення сеансового ключа Опис алгоритму та приклад розрахунку Двоключовий алгоритм шифрування над еліптичною кривою. Опис алгоритму та приклад розрахунку Двоключовий алгоритм цифрового підпису над еліптичною кривою. Опис алгоритму та приклад розрахунку.

Тема 3.	***Криптоаналіз поточних шифрів.*** Регістри зсуву з лінійним (РЗЛЗЗ) та нелінійним (РЗНЗЗ) зворотнім зв'язком, причина непридатності для шифрування регістрів з нелінійним зворотнім зв'язком, зв'язок довжини регістру з максимальною довжиною послідовності, що не повторюється, поняття лінійної складності. Примітивний пов'язаний з регістром багаточлен – необхідна умова генерації послідовності максимальної довжини. Яку довжину послідовності слід перехопити, щоб зламати шифр на ґрунті РЗЛЗЗ. Побудова системи лінійних рівнянь та рішення системи – спосіб зламати шифр на ґрунті РЗЛЗЗ
Тема 4.	***Криптоаналіз двоключових криптосистем за допомогою факторизації*** Особливості обрання параметрів двоключові криптосистеми, які впливають на стійкість. Поняття сильних простих чисел, та первообразних коренів у полях Галуа. Функція Ейлера як секретний параметр криптосистеми. Вплив цих характеристик на криптостійкість. Приклади атак на не стійку реалізацію алгоритму RSA.Атака на ключ RSA та методи факторизації: повний перебор, P-1 метод Полларда, ро метод Полларда, лямда метод Полларда, метод решета у числовому полі, відомості про квантовий алгоритм Шора. Приклади розрахунку в таких атаках та оцінювання складності атаки.
Тема 5.	***Криптоаналіз двоключових криптосистем за допомогою дискретного логарифмування*** Особливості обрання параметрів двоключові криптосистеми, які впливають на стійкість. Поняття сильних простих чисел, та первообразних коренів у полях Галуа. Метод Поліга-Хеллмана як універсальний метод пошуку дискретних логарифмів. Вплив цих характеристик на криптостійкість. Приклади атак на не стійку реалізацію алгоритму Діффі-Хеллмана. Атака на ключ RSA та методи пошуку дискретного логарифму: повний перебор, «кроки немовля – кроки велетня», ро метод Полларда, лямда метод Полларда, відомості про квантовий алгоритм Шора. Приклади розрахунку в таких атаках та оцінювання складності атаки. Дискретне логарифмування над еліптичною кривою та атака на шифр методом «кроки немовля – кроки велетня»
Тема 6	***Диференціальний криптоаналіз симетричних шифрів*** Загальна схема атаки на симетричний шифр. Поняття диференциалу, методик розрахунку диференціалів, приклад диференціального криптоаналізу одного етапу шифру DES та трьох етапів.
Тема 7	***Лінійний криптоаналіз сиетричних шифрів*** Загальна схема атаки на симетричний шифр. Поняття ефективного лінійного статистичного аналогу нелінійних перетворень, приклад лінійного криптоаналізу одного етапу шифру DES та чотирьох етапів
Тема 8	***Лінійно-диференціальний криптоаналіз симетричних шіфрів*** Загальна схема атаки на симетричний шифр. Методика комбінування лінійного та диференціального криптоаналізу. Приклад лінійно-диференціального криптоаналізу на 7 та 8 етапів шифру DES

Список рекомендованих джерел

1. Shannon C.E. Communication theory of secrecy systems // The Bell System Technical Journal – 1949 – Volume: 28, Issue: 4.
2. Smart Nigel Cryptography: An Introduction, 3rd Edition.–A McGraw Hill Publication., 2003

3. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C: 20th Anniversary Edition. Wiley, 2015. 784 p.
4. Stavroulakis P., Stamp M. Handbook of Information and Communication Security. Berlin: Springer-Verlag, 2010. 863 p.
5. ДСТУ ISO/IEC 9798.
6. ДСТУ ISO/IEC 15946.
7. Рекомендації X.800.

Інформація про консультації

Кожного понеділка у вересні-листопаді 2023 року з 15^{00} до 16^{20} год., дистанційно. Ст. викл. Басов В. Є.

Загальна схема оцінювання

Сума балів за всі види навчальної діяльності	Шкала ЄКТС	Оцінка за національною шкалою		Нарахування балів	Бали нараховуються таким чином:
		для іспиту	для заліку		
90-100	A	Відмінно	Зараховано		***Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою*** і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів, за результати екзамену – до 40 балів.
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		

Політика опанування дисципліни

Відвідування: Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях та контрольних заходах (екзамен/залік) є обов'язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.
Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **Unicheck.**
Умови зарахування пропущених занять:
Інші умови: Навчально-методичні матеріали дисципліни розміщені на платформі Moodle.