Волинський національний університет імені Лесі Українки

Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
нормативної навчальної дисципліни

Математичні основи криптографії

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Інформаційна безпека (2020)
Форма навчання	Денна
Розробник (викладач)	Жигаревич Оксана Костянтинівна, старший викладач
Контактна інформація	Електронна адреса викладача: Zhyharevych.Oksana@vny.edu.ua
Програма навчальної дисципліни	Програма навчальної дисципліни розміщена на сторінці кафедри комп'ютерних наук та кібербезпеки на офіційному сайті ВНУ імені Лесі Українки
Семестр, курс	3 семестр, 2 курс
Обсяг дисципліни	Загальний обсяг: 4,5 кредити / 135 годин. Аудиторних годин: 64; з них: лекцій – 32 год., лабораторних – 32 год. Самостійної роботи: 63 год. Консультації: 8 год.
Форма контролю	екзамен
Час занять	Тижневих годин – 3,5 год. Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Анотація дисципліни	Дисципліна «Математичні основи криптографії» належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра за спеціальністю 125 «Кібербезпека». Вивчається як окремий розділ криптографії та спрямована на вивчення методів отримання вихідного значення зашифрованої інформації за допомогою математичних методів, не маючи доступу до секретної інформації (ключа), необхідної для цього.

Предреквізити дисципліни	Дисципліна є логічним продовженням предметів: «Математичний аналіз», «Програмування». Для вивчення будуть корисні знання та вміння отримані з дисциплін «Криптоаналіз», «Технології програмування захищених систем», «Теорія інформації та кодування» та ін.
Постреквізити дисципліни	Знання та вміння, отримані в результаті вивчення дисципліни, можуть бути використані для написання курсової роботи з навчальних дисциплін циклу професійної підготовки, а також у професійному розвитку та роботі розробляти і застосовувати криптографічні алгоритми та протоколи для захисту інформації; реалізовувати системи захисту інформації в інформаційних і комунікаційних системах; застосовувати методи і засоби запобігти звичайному перехопленню даних.
Мета вивчення дисципліни	Мета дисципліни: розглянути класичні та сучасні математичні методи криптографії; класифікацію, характеристики, приклади та типи криптоатак; навчитися досліджувати математичні алгоритми криптології, виконувати криптоаналіз класичних шифрів, оцінювати слабкі та сильні сторони шифрів, аналізувати процес дешифрування.
Навчальна логістика	1. Загальні проблеми захисту інформації. 2. Предмет криптології. 3. Історія створення криптології. 4. Математичні основи криптології. 5. Основи класичної криптології. 6. Шифри з відкритим ключем. 7. Електронний підпис. 8. Стандарт підпису DSA (DIGITAL SIGNATURE ALGORITM).\ 9. Криптографічні протоколи. 10. Електронні грошові одиниці.

Результати навчання	1. Здатність застосовувати знання у практичних ситуаціях. (ЗК 1). 2. Знання та розуміння предметної області та розуміння професії. (ЗК 2). 3. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. (ЗК4). 4. 5Здатність до пошуку, оброблення та аналізу інформації. (ЗК 5). 5. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. (ФК 10). 6. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібезбезпеки. (ФК 12). 7. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. (ПРН 47) 8. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. (ПРН 48)
Загальні компетентності	ЗК 2. Здатність до абстрактного мислення, аналізу та синтезу. ЗК 3. Здатність застосовувати знання у практичних ситуаціях. ЗК 4. Здатність планувати та управляти часом. ЗК 5.Знання та розуміння предметної області та розуміння професійної діяльності. ЗК 6. Здатність спілкуватися державною мовою як усно, так і письмово ЗК 7. Навички використання інформаційних і комунікаційних технологій. ЗК 8. Здатність вчитися і оволодівати сучасними знаннями. ЗК 9. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК 10. Вміння виявляти, ставити та вирішувати проблеми. ФК 1. Здатність виявляти внутрішні та зовнішні загрози, умови, джерела походження та граничні показники (індикатори безпеки) економічної, екологічної, військової, цивільної безпеки. ФК 2. Здатність моніторити розвиток загроз, оцінювати їх можливі наслідки, давати експертизу рішень, що приймається з точки зору безпеки. ФК 3. Здатність формувати та вдосконалювати нормативно-правову базу та моделі безпеки для протидії загрозам. ФК 4. Здатність формувати та вдосконалювати організаційні структури та створювати відповідні умови для забезпечення безпеки. ФК 5. Здатність розробляти та проводити загальні і спеціальні

	заходи з безпеки, які реалізуються в усіх напрямах і видах діяльності суб'єктів господарювання. ФК15. Здатність ефективно працювати із засобами масової інформації. ФК16. Здатність забезпечити безпечне середовище у сфері економіки, екології та інформаційної безпеки.

Оцінювання

Оцінювання навчальних досягнень з дисципліни "Математичні основи криптографії" здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах, вчасне і якісне виконання домашніх завдань) та модульний контроль (оцінюються модульні контрольні роботи у вигляді тестів або письмово або у вигляді індивідуальних завдань). Максимальна кількість балів, яку може заробити студент під час поточного оцінювання за семестр – 40 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за всі модульні контрольні роботи (МКР). Максимальна кількість балів, яку може заробити студент під час модульного контролю за семестр складає 60 балів. Додаткові бали (бонусні, які можуть замінити бали за інший вид робіт) студенти можуть отримати написавши тези (статтю) на конференцію згідно тем предмету, але за умови, що тези прийняли та опублікували, а викладач надав свій позитивний відгук.

Якщо студент за період вивчення дисципліни набрав за поточний та модульний контроль мінімум 60 балів і погоджується із цим результатом, то оцінка за семестр може виставлятися без складання заліку. В іншому випадку студент складає залік; максимальна кількість балів, яку можна отримати на заліку – 60 балів. Оцінка за семестр, у випадку складання заліку, є сумою балів поточного контролю та балів, отриманих під час заліку.

Політика викладача щодо студента

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загально-прийнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування. Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу.

Політика щодо академічної доброчесності

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Порушенням академічної доброчесності вважається: академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування. За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності: повторне проходження оцінювання; повторне проходження відповідного освітнього компонента освітньої програми.

Під час модульного та підсумкового контролю (заліку) студентам заборонено користуються такими засобами як мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси.

Політика щодо дедлайнів та перескладання

Усі передбачені завдання мають бути виконані у встановлений термін. Несвоєчасно виконані завдання оцінюються на нижчу оцінку. Виключенням можуть бути завдання, які не

вдалося зробити з поважних причин, в такому випадку студент може доробити вказані завдання у вказаний термін.

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, то він (вона) вивчає матеріал самостійно, використовуючи навчальні посібники, конспекти лекцій, матеріали дистанційного курсу, у випадку розміщення його на платформі дистанційного навчання Moodle, виконує всі домашні завдання. Прозвітуватися про виконання завдань можна, використовуючи дистанційний курс, прикріпивши виконанні завдання у відповідні комірки та попередити викладача про здане завдання, або під час консультацій або надіслати виконане завдання на корпоративну пошту викладача. Зворотній зв'язок з викладачем для з'ясування всіх питань: використання форуму, чату дистанційного курсу, корпоративної пошти університету або відповідної бесіди у певному месенджері.

Перескладання модульного контролю (письмового чи тестування) заборонено.

Рекомендована література

1. Криптоанализ и криптография: история противостояния. [Електронний ресурс]. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/kriptoanaliz-i-kriptografiya-istoriya- protivostoyaniya/viewer
2. Анализ симметричных криптосистем. [Електронний ресурс]. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/analiz-simmetrichnyh-kriptosistem/viewer
3. Шнайер Б. Прикладная криптография, 2-е издание, Протоколы, алгоритмы и исходные тексты на языке С. – М.: "Триумф", 2001. – 610 с.
4. Baigneres, T. A Classical Introduction to cryptography Exercise Book [Text] / T. Baigneres, P. Junod, Y. Lu, J. Monneart, S. Vaudenay. – Springer, 2006. – 254 p.
5. Hoffstein, J. An Introduction to Mathematical Cryptography [Text] / J. Hoffstein, J. Pipher, J.H. Silverman. – Springer, 2008. – 523 p.
6. Menezes, A. J. The Handbook of Applied Cryptography [Text] / A. J. Menezes, P. K. Oorschot, S. A. Vanstone. – New York: CRC Press, 1997. – 816 c.
7. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications [Text]: NIST Special Publication 800-22 Rev1. – Gaithersburg, Maryland: NIST, 2008. – 153 p.
8. Криптологія: навч.-метод. посіб. / Людмила Ярославівна Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с
9. Криптологія у прикладах, тестах і задачах: навч. посібник / Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомичова. – Д.: Національний гірничий університет, 2013. 318 с.
10. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Людмила Ярославівна Глинчук – Луцьк: РВВ "Вежа" Волин. нац. ун-т ім. Лесі Українки, 2014. – с. 186
11. Основы криптоанализа. [Електронний ресурс]. – Режим доступу до ресурсу: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema18

Затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 2 від 15 вересня 2021 р.

Завідувача кафедри _____ Гришанович Т.О.