Волинський національний університет імені Лесі Українки

Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативної навчальної дисципліни

Криптоаналіз

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Інформаційна безпека (2020)
Форма навчання	Денна
Розробник (викладач)	Глинчук Людмила Ярославівна, кандидат фізико-математичних наук
Контактна інформація	Електронна адреса викладача: Hlynchuk.Ludmila@vnu.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	6 семестр, III курс
Обсяг дисципліни	Загальний обсяг: 4 кредити / 120 годин. Аудиторних годин: 60; з них: лекцій – 28 год., лабораторних – 32 год. Самостійної роботи: 52 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 «Криптоаналіз» належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра за спеціальністю 125 «Кібербезпека». Вивчається як окремий розділ криптології та спрямована на вивчення методів отримання вихідного значення зашифрованої інформації, не маючи доступу до секретної інформації (ключа), необхідної для цього. Цікавим є сам процес дешифрування та необхідні ресурси та знання, які потрібно використати, а також, можливість оцінити сильні та слабкі сторони методів шифрування
Предреквізити дисципліни	Дисципліна є логічним продовженням предметів: «Математичні основи криптографії», «Криптографічний та стеганографічний захист інформації». Для вивчення будуть корисні знання та вміння отримані з дисциплін «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.
Мета вивчення дисципліни	Мета дисципліни: розглянути класичний та сучасний криптоаналіз; основні та додаткові методи криптоаналізу; класифікацію, характеристики, приклади та типи криптоатак; навчитися досліджувати алгоритми криптоаналізу, виконувати криптоаналіз класичних шифрів, оцінювати слабкі та сильні сторони шифрів, аналізувати процес дешифрування.
Що буде вивчатись	1. Історія криптоаналізу та загальні відомості. 2. Особливості криптографічної стійкості різних методів шифрування. Теоретична та практична стійкість шифру. Абсолютна стійкість. 3. Класичний криптоаналіз та сучасний криптоаналіз. 4. Основні методи криптоаналізу для симетричних криптосистем. 5. Основні методи криптоаналізу для асиметричних криптосистем 6. Додаткові методи криптоаналізу. 7. Класифікація та типи криптоатак. 8. Дешифрування шифру простої заміни. 9. Дешифрування шифру перестановки. 10. Приклади криптоаналізу відомих класичних шифрів. 11. Моделі загроз безпеки криптосистем. 12. Показники стійкості, продуктивності та зручність реалізації алгоритмів. 13. Особливості програмної реалізації криптоаналізу. Приклади. 14. Апаратна складова криптоаналізу. Пристрої, їх особливість та ефективність.
Результати навчання	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. 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. РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. РН 12. Розробляти моделі загроз та порушника. Та інші.

Оцінювання

Оцінювання навчальних досягнень з дисципліни “Криптоаналіз” 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.

Якщо студент за період вивчення дисципліни набрав за поточний та модульний контроль мінімум 75 балів і погоджується із цим результатом, то оцінка за семестр може виставлятися без складання екзамену. В іншому випадку студент складає екзамен; максимальна кількість балів, яку можна отримати на екзамені – 60 балів. Оцінка за семестр, у випадку складання екзамену, є сумою балів поточного контролю та балів, отриманих під час екзамену.

Політика викладача щодо студента

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загальноприйнятих 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. Методи криптоаналізу. Курс відео-лекцій (Лектор: проф. Антон Миколайович Олексійчук) [Електронний ресурс]. – Режим доступу до ресурсу: https://www.youtube.com/watch?v=GHsfv8LygWY&list=PLhCN8H4P5Lvg0jAzaN_iiWaBib

QMMI2vy&ab_channel=%D0%9A%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B0%D0%9C%D0%9C%D0%97%D0%86
2. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Людмила Ярославівна Глинчук – Луцьк: РВВ “Вежа” Волин. нац. ун-т ім. Лесі Українки, 2014. – с. 186
3. Основы криптоанализа. [Електронний ресурс]. – Режим доступу до ресурсу: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema18
4. Шнайер Б. Криптоанализ // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — С. 19—22. — 816 с. — 3000 экз. — ISBN 5-89392-055-4.
5. Криптоанализ RSA. [Електронний ресурс]. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/kriptoanaliz-rsa/viewer
6. Криптоанализ и криптография: история противостояния. [Електронний ресурс]. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/kriptoanaliz-i-kriptografiya-istoriya-protivostoyaniya/viewer
7. Анализ симметричных криптосистем. [Електронний ресурс]. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/analiz-simmetrichnyh-kriptosistem/viewer
8. Блочные шифри и их криптоанализ. [Електронний ресурс]. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/blochnye-shifry-i-ih-kriptoanaliz/viewer