Волинський національний університет імені Лесі Українки

Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

вибіркової навчальної дисципліни

Основи криптографічного захисту

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	122 Комп'ютерні науки
Освітня програма	Комп'ютерні науки та інформаційні технології (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	8 семестр, IV курс
Обсяг дисципліни	Загальний обсяг: 4 кредити / 120 годин. Аудиторних годин: 40; з них: лекцій – 20 год., практичних – 20 год. Самостійної роботи: 72 години.
Форма контролю	Залік
Час занять	Тижневих годин – 3 год. Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Анотація дисципліни	Дисципліна «Основи криптографічного захисту» спрямована на вивчення основних понять та напрямів криптографічного захисту: симетричних та асиметричних алгоритмів (методів) шифрування, їх використання, цифрового підпису, хеш-функції, криптопротоколів, криптовалюти, законодавства у сфері криптографічного захисту та видів криптоаналізу і можливість його застосування. Предметом вивчення дисципліни є забезпечення формування знань та вмінь, що необхідні для вирішення професійних завдань.
Пререквізити дисципліни	Базові знання з дисциплін: «Теорія ймовірностей та математична статистика», «Алгебра та геометрія». Базові знання з тем «Системи числення», «Модульна арифметика» та ін.
Постреквізити дисципліни	Знання та вміння, набуті в результаті вивчення дисципліни можна використати при поглибленому вивченні кожного з напрямів

	криптографії, криптології, стеганографії, криптоаналізу, захисту інформації та ін. А також, для написання випускних кваліфікаційних робіт (бакалаврської, магістерської).
Мета вивчення дисципліни	Мета дисципліни полягає в - ознайомленні із загальними поняттями та історією розвитку криптології; із симетричними та асиметричними методами шифрування; з основними напрямками використання криптографічних методів; з програмним та апаратним забезпечення на основі криптографічного захисту; з особливостями та використанням цифрового підпису, хеш-функції, криптопротоколів; криптографією на еліптичних кривих, з основними поняттями криптовалюти та її поширення у світі; з основами криптоаналізу; із законодавством у сфері криптографії; - формуванні у студентів знань та умінь, які створять теоретичний і практичний фундамент, необхідний для аналізу необхідності застосування того чи іншого методу шифрування, апаратного чи програмного засобу, а також можливість виконувати простий криптоаналіз і оперувати відповідним законодавством.
Що буде вивчатись	1. Криптологія: основні поняття та історичний розвиток. Основні напрями розвитку. 2. Нормативно-правове регулювання у галузі криптографічного захисту інформації. 3. Найпростіші класичні шифри: перестановки, заміни, гамування та ін. 4. Симетричні стандарти шифрування DES, ГОСТ. 5. Асиметрична криптографія. Алгоритм RSA, система Діффі-Хелмана та Ель-Гамаля. 6. ЕЦП та хеш-функції. Застосування та приклади. 7. Поняття про криптопротоколи. Криптографія на еліптичних кривих. 8. Криптовалюта: виникнення, поширення та використання. 9. Програмна та апаратна реалізація алгоритмів шифрування (приклади). 10. Загальні поняття криптоаналізу: типи, види та особливості.
Результати навчання	1. Здатність застосовувати знання у практичних ситуаціях. 2. Здатність вчитися й оволодівати сучасними знаннями. 3. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. 4. Розуміти принципи та суть криптографічного захисту інформації. Знати основний поділ методів шифрування та основні криптографічні алгоритми, їх характеристики, базові стандарти в галузі криптографічного захисту інформації. 5. Здатність застосовувати засоби криптографічного захисту та визначати необхідність застосування. Здійснювати загальну оцінку якості криптографічного захисту інформації в системах зберігання, передавання та обробки інформації.

Оцінювання

Оцінювання навчальних досягнень з дисципліни “Основи криптографічного захисту” 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, 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. Фергюсон, Нильс, Шнайер, Брюс. Практическая криптография.: Пер. с англ. – М.: Издательський дом «Вильямс», 2005. – 424 с.: ил. – Парал. тит. англ. ISBN 5-8459-0733-0 (рус.)
2. Романьков В.А. Введение в криптографию. Курс лекций. 2-е изд., исправ. – М.: ФОРУМ, 2012. – 240 с. – (Высшее образование). – ISBN: 9785911345730
3. Ященко В.В. Введение в криптографию. Под общей ред. В. В. Ященко. – 4 изд., доп. – М.: МЦНМО, 2012. – 348 с. – ISBN 978-5-4439-0026-1.
4. Глинчук Л. Я. Криптологія: навч.-метод. посіб. / Л. Я. Глинчук. – Луцьк: Вежа-Друк, 2014. – 164 с.
5. Глинчук Л.Я. Дистанційний курс «Основи криптографічного захисту інформації» [Електронний ресурс]. – Режим доступу до ресурсу: http://194.44.187.60/moodle/course/view.php?id=796
6. Глинчук Л.Я. База тестів для модульного контролю з курсу «Основи криптографічного захисту інформації». Посилання видається за 5 хв. до проходження тестів.
7. Основы криптографии. Часть 1. [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=t7kNtZ94u-Y&list=PL_8BBd8_xXlaRxaF8cianF8K4-zpd6mjG&index=2
8. Основы криптографии. Часть 2. [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=mlMcNWTwxMw&list=PL_8BBd8_xXlaRxaF8cianF8K4-zpd6mjG&index=1
9. Классическая Криптография. [Електронний ресурс]. – Режим доступу: https://www.youtube.com/playlist?list=PLbnf75Jro21rz_PuugcnX3O3HYPfBPdc8

Затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 7 від 5 січня 2021 р.

В. о. завідувача кафедри _____ Гришанович Т.О.