Волинський національний університет імені Лесі Українки

Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

вибіркової навчальної дисципліни

Програмування криптографічних алгоритмів та протоколів

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	8 семестр, IV курс
Обсяг дисципліни	Загальний обсяг: 6,5 кредитів / 195 годин. Аудиторних годин: 50; з них: лекцій – 22 год., практичних – 28 год. Самостійної роботи: 139 год.
Форма контролю	Залік
Час занять	Тижневих годин – 4,5 год. Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Анотація дисципліни	Дисципліна «Програмування криптографічних алгоритмів та методів» є практичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки з питань забезпечення криптографічного захисту інформації. Дисципліна є логічним та практичним продовженням дисципліни «Основи криптографічного захисту інформації» та дає можливість глибше зрозуміти не тільки суть криптографічних алгоритмів та протоколів за їх основним поділом, але і набути практичних навичок програмування математичних моделей криптографії.
Предреквізити дисципліни	Базові знання з дисциплін: «Теорія інформації та кодування», «Математичні основи криптографії», «Вступ до програмування». Базові знання з тем «Системи числення», «Модульна арифметика» та ін.

Постреквізити дисципліни	Знання та вміння, набуті в результаті вивчення дисципліни, можна використати для написання випускної кваліфікаційної роботи.
Мета вивчення дисципліни	Метою викладання дисципліни є надання студентам системних знань з принципів побудови та програмування систем криптографічного захисту інформації, освоєння ними необхідних знань та отримання навиків з організації та забезпечення захисту інформації в інформаційно-телекомунікаційних системах. Завданнями вивчення навчальної дисципліни є володіння основами засобів криптографічного захисту інформації, практичними навичками проектування та програмування алгоритмів та протоколів криптографічних перетворень, основними способами шифрування даних.
Що буде вивчатись	1. Повторення: суть, особливості та основні напрями криптографії. Модель криптографічної системи. 2. Програмування найпростіших класичних шифрів: перестановки, заміни, гамування та ін. 3. Програмування певних блоків симетричних стандартів шифрування: DES, ГОСТ, AES. 4. Програмування асиметричних алгоритмів: RSA, система Діффі-Хелмана та Ель-Гамаля. 5. Програмування хеш-функцій. 6. Класифікація криптографічних протоколів, безпека та атаки. 7. Аналіз та моделювання криптографічних протоколів. 8. Програмування протоколів ЕЦП. 9. Програмування протоколів, що ґрунтуються на симетричних криптосистемах. 10. Програмування протоколів, що ґрунтуються на асиметричних криптосистемах. 11. Квантовий розподіл ключів: протокол BB84, протокол B92, протокол E91 (EPR). Протокол розподілу ключів, що ґрунтується на кодуванні через часові зсуви. 12. Протокол розподілу ключів за допомогою еліптичних кривих.
Результати навчання	1. Здатність застосовувати знання у практичних ситуаціях. 2. Знання та розуміння предметної області та розуміння професії. 3. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. 4. Здатність до пошуку, оброблення та аналізу інформації. 5. Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності. 6. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. 7. Програмувати криптографічні методи та протоколи, а також використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

Оцінювання

Оцінювання навчальних досягнень з дисципліни “Програмування криптографічних алгоритмів та протоколів” 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. 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. / Людмила Ярославівна Глинчук. – Луцьк: Вежа-Друк, 2014. – 164 с.
5. Технології захисту інформації [Електронний ресурс]: підручник для студ. спеціальності 122 «Комп’ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
6. Аграновский А.В., Хади Р.А. Практическая криптография: алгоритмы и их программирование. – М.: СОЛОН-Пресс, 2002. – 256 с.
7. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК Пресс, 2012. – 256 с.

Затверджено на засіданні кафедри комп’ютерних наук та кібербезпеки

протокол № 7 від 5 січня 2021 р.

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