Волинський національний університет імені Лесі Українки

Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативної навчальної дисципліни

Технології захисту інформації

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	01 Середня освіта
Спеціальність	014 Середня освіта (Інформатика)
Освітня програма	Середня освіта. Інформатика (2021)
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: 36; з них: лекцій – 20 год., лабораторних – 30 год. Самостійної роботи: 62 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 «Технології захисту інформації» належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра. Є теоретичною та практичною основою сукупності знань та вмінь та виступає однією з головних у формуванні знань у студентів з питань забезпечення захисту інформації та формування політики безпеки.
Предреквізити дисципліни	Базові знання з дисциплін: «Вища математика», «Програмування», «Прикладне програмне забезпечення а хмарні технології», «Теорія ймовірностей та математична статистика», «Системне програмування та операційні системи», «Комп'ютерні мережі та інтернет-технології».

Постреквізити дисципліни	Знання та вміння, набуті в результаті вивчення дисципліни, можна використати у подальшому навчанні та у професійній діяльності. А також, для написання індивідуальних, курсових та випускних кваліфікаційних робіт (бакалаврської, магістерської).
Мета вивчення дисципліни	**Метою** викладання навчальної дисципліни «Технології захисту інформації» є надання студентам системних знань з принципів побудови систем криптографічного захисту інформації, освоєння ними необхідних знань та отримання навиків з організації та забезпечення захисту інформації в інформаційно-телекомунікаційних системах. **Завдання:** основними завданнями вивчення дисципліни "Технології захисту інформації" дати наступні **знання**: про життєвий цикл розробки систем безпеки; стандарти безпеки, механізми та політики розмежування прав доступу; основні методи крипрографічного захисту; основні види атак, загроз та тестування на проникнення; методи та засоби забезпечення інформаційної безпеки в ОС, мережі, пам'яті **та вміння**: використовувати методи і засоби захисту в ОС, мережі і т.д.; орієнтуватись у системі нормативно-правових документів захисту інформації; застосовувати розмежування прав, політики доступу та механізми контролю, паролі; використовувати засоби крипрографічного захисту.
Що буде вивчатись	1. Огляд безпеки системи. Законодавство у сфері захисту України. 2. Механізми і політики розмежування прав доступу. Стандарти. 3. Шифрування даних. 4. Алгоритми із секретним ключем. 5. Алгоритми з публічним ключем. 6. Цифрові підписи. 7. Основні види атак, принципи криптоаналізу. Тестування на проникнення. 8. Методи та пристрої забезпечення інформаційної безпеки. 9. Моделі захисту. Захист пам'яті. 10. Використання паролів і механізмів контролю за доступом (Захист в ОС).
Результати навчання	Відповідно до таблиць ОПП спеціальності 014, 2021 р. ЗК 6, 9, 10, 11 СК 1, 2, 3, 5, 8, 12, 15, 16, 17, 23, 25 ПРН 2, 4, 10, 13, 22, 23, 25

Оцінювання

Оцінювання навчальних досягнень з дисципліни "Технології захисту інформації" 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. Тарнавський Ю. А. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки»; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.
2. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.).

3. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020. – 678 с.
4. Карачка А. Ф. Технології захисту інформації. Текст лекцій. – Тернопіль: ТНЕУ, 2017. – 86 с.
5. Дистанційний курс «Основи інформаційної безпеки». [Електронний ресурс]. – Режим доступу: https://courses.prometheus.org.ua/courses/KPI/IS101/2014_T1/about
6. Дистанційний курс «Інформаційна гігієна. Як розпізнати брехню в соцмережах, в інтернеті та на телебаченні». [Електронний ресурс]. – Режим доступу: https://courses.prometheus.org.ua/courses/course-v1:Prometheus+IH101+2021_T3/about
7. Серіал для батьків «Безпека дітей в інтернеті»/ Дистанційний курс. [Електронний ресурс]. – Режим доступу: https://osvita.diia.gov.ua/courses/serial-dlya-batkiv-onlayn-bezpeka-ditey
8. Серіал для батьків «Кіберняні»/ Дистанційний курс. [Електронний ресурс]. – Режим доступу: https://osvita.diia.gov.ua/courses/cybernanny
9. Серіал для батьків «Основи кібергігієни»/ Дистанційний курс. [Електронний ресурс]. – Режим доступу: https://osvita.diia.gov.ua/courses/cyber-hygiene
10. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – КІІВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с. [Електронний ресурс]. – Режим доступу до ресурсу: http://dspace.onua.edu.ua/bitstream/handle/11300/11111/%D0%9E%D0%86%D0%91%20%D0%BA%D0%BE%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%20%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D0%B9.pdf?sequence=1&isAllowed=y
11. Інформаційна безпека : рекомендаційний покажчик / уклад.: С. Л. Бондар, Т. А. Сіденко. – Чернігів : Наукова бібліотека НУ «Чернігівська політехніка», 2020. – 44 с.

Затверджено на засіданні кафедри комп’ютерних наук та кібербезпеки
протокол № 2 від 15 вересня 2021 р.

В. о. завідувача кафедри  Гришанович Т.О.