



Прийкарпатський
національний
університет імені
Василя Стефаника



Кафедра
математики та
інформатики і
методики
навчання

СИЛАБУС
Навчальної дисципліни
«Захист інформації»

Розробник Кланічка Юрій Володимирович, кандидат фізико-математичних наук, доцент кафедри математики та інформатики і методики викладання
yuriy.klanichka@pnu.edu.ua

Загальна інформація

Освітня програма	Середня освіта (Інформатика)
Спеціальність	014 Середня освіта
Спеціалізація	014.04 Середня освіта (Інформатика)
Галузь знань	01 Освіта/Педагогіка
Рівень вищої освіти	Перший (бакалаврський)
Статус дисципліни	Вибіркова
Мова викладання	Українська
Обсяг дисципліни	3 кредити ECTS/90 год. Лекції – 14 год. Лабораторні заняття – 16 год. Самостійна робота – 60 год.
Курс / семестр	2 курс /3 семестр
Підсумковий контроль	Залік Курс проектно-орієнтований, підсумок проводиться у вигляді захисту портфоліо робіт за семестр.

Опис дисципліни

Мета	Мета курсу: Метою вивчення навчальної дисципліни «Захист інформації» є ознайомлення з принципами побудови та використання програмних та програмно-апаратних засобів для захисту програмного забезпечення та іншої інформації в комп'ютерних системах, використання основних принципів побудови систем захисту інформації та методів протидії спробам несанкціонованого доступу до неї з боку сторонніх осіб. Завданням дисципліни є формування у студентів теоретичних знань та вироблення практичних навичок проектування комплексних рішень із захисту інформації в комп'ютерних системах.
Результати навчання	ПР 3. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.

	<p>ПР 4. Проводити системний аналіз об'єктів проектування та обґрунтовувати вибір структури, алгоритмів та способів передачі інформації в інформаційних системах та технологіях.</p>
Зміст дисципліни	<p>Тема 1. Складові «Інформаційної безпеки». Огляд безпеки системи. Методи та пристрої забезпечення захисту і безпеки</p> <p>Тема 2. Захист, доступ та автентифікація. Шифрування файлів. Моделі захисту інформації</p> <p>Тема 3. Відновлення даних. Антивірусний захист.</p> <p>Тема 4. Механізми та Протоколи керування ключами в ІВК інформаційної системи. Шифрування даних.</p> <p>Тема 5. Основні види атак, принципи риптоаналізу.</p> <p>Тема 6. Алгоритми з секретним ключем. Алгоритми з відкритим ключем.</p> <p>Тема 7. Протоколи автентифікації. Поточкові шифри. Хешування. Цифрові підписи.</p>
Загальна система оцінювання курсу	<p style="text-align: center;">Теоретична підготовка</p> <p style="text-align: center;">Високий, А, 91* – 100, відмінно - 5</p> <p>Студент має глибокі, міцні і систематичні знання всіх положень наукової методології, може не тільки вільно матеріалом, але й самостійно довести існування певних закономірностей, принципів, використовує здобуті знання і вміння в нестандартних ситуаціях, здатний вирішувати проблемні питання. Відповідь студента відрізняється точністю формулювань, логікою, достатній рівень узагальненості знань</p> <p style="text-align: center;">Вище середнього, середній В, С, 81 – 90; 71 – 80; дуже добре, добре - 4</p> <p>Студент знає і може самостійно сформулювати основні методологічні підходи, принципи їх застосування, , але не завжди може самостійно здійснити критичний аналіз. Студент може самостійно застосовувати знання в стандартних ситуаціях, його відповідь логічна, але розуміння не є узагальненим.</p> <p style="text-align: center;">Достатній, D, E, 61 – 70, 51 - 60 задовільно, посередньо - 3</p> <p>Студент відтворює основні поняття і визначення курсу, але досить поверхово, не виділяючи взаємозв'язок між ними, може сформулювати з допомогою викладача основні методологічні положення, знає істотні ознаки (засади) основних підходів та їх відмінність, може записати окремі термінологічні дефініції теоретичного положення за словесним формулюванням і навпаки; допускає помилки, які повною мірою самостійно виправити не може.</p> <p style="text-align: center;">Низький, FX / F 1 – 51, незадовільно 2</p> <p>Відповідь студента при відтворенні навчального матеріалу елементарна, фрагментарна, зумовлена нечіткими уявленнями про закони і методи. У відповіді цілком відсутня самостійність. Студент знайомий лише з деякими основними поняттями та визначеннями змістовного модуля, з допомогою викладача може сформулювати лише деякі основні положення теорії.</p>
Вимоги до письмової роботи	<p style="text-align: center;">Високий, А, 91* – 100, відмінно - 5</p> <p>Студент самостійно розв'язує типові ситуаційні задачі захисту інформації різними способами - стандартними, комбінованими й нестандартними, здатний проаналізувати й узагальнити отриманий</p>

	<p>результат. При виконанні індивідуальних завдань та самостійних робіт студент дотримується усіх вимог, передбачених програмою курсу. Крім того, його дії відрізняються раціональністю, вмінням оцінювати помилки й аналізувати результати</p> <p>Вище середнього, середній В, С, 81 – 90; 71 – 80; дуже добре, добре - 4</p> <p>Студент самостійно розв'язує типові завдання, володіє базовими навичками з виконання необхідних логічних операцій, може самостійно скласти типову схему та обрати раціональний метод, але не завжди здатний провести аналіз і узагальнення результату.</p> <p>Достатній, D, E, 61 – 70, 51 - 60 задовільно, посередньо - 3</p> <p>Студент може сформулювати найпростіший захист інформації за зразком, виявляє здатність виконувати основний елементарний її аналіз, але не спроможний самостійно сформулювати і визначити метод її роботи. При вирішенні фабули студент виконує роботу за зразком, але з помилками робить висновки, не розуміє достатньою мірою мету роботи.</p> <p>Низький, FX / F 1 – 51, незадовільно 2</p> <p>Студент знає основні терміни але не вміє сформулювати окремих захист інформації. Не здатний виконувати основний елементарний аналіз захисту інформації, не спроможний самостійно сформулювати і визначити метод її роботи. Студент виконує роботу за зразком, але з помилками робить висновки, не розуміє достатньою мірою мету роботи.</p>
Семінарські заняття	-
Умови допуску до підсумкового контролю	<p>Студент допускається до складання заліку, якщо впродовж семестру він за змістові модулі набрав сумарно 25 балів і вище.</p> <p>Студент не допускається до складання заліку, якщо впродовж семестру він за змістові модулі набрав менше 25 балів. У цьому випадку студенту у відомості робиться запис "не допущений" і виставляється набрана кількість балів. Допускається, як виняток, з дозволу декана факультету за заявою, погодженою з відповідною кафедрою, одноразове виконання студентом додаткових видів робіт з навчальної дисципліни (відпрацювання пропущених занять, перескладання змістових модулів, виконання індивідуальних завдань тощо) для підвищення оцінок за змістові модулі.</p> <p>Напередодні заліку викладач подає доповідну декану про недопуск студентів академічної групи (груп). Відмітка про недопуск у відомості робиться при наявності розпорядження декана.</p>
Організація навчання	<p style="text-align: center;">Особливості навчання</p> <p>Синхронна комунікація відбувається згідно розкладу занять – стаціонарно або дистанційно - у віртуальній кімнаті Meet, вхід у яку є доступний у класі.</p> <p>Весь навчально - методичний комплекс дисципліни розміщено на сайті дистанційного навчання.</p> <p>Асинхронна комунікація здійснюється у класі впродовж усього процесу вивчення дисципліни, в межах робочого часу.</p> <p>Організація навчання здійснюється у віртуальному класі Google Classroom в домені pnu.edu.ua. В класі постійно доступні усі необхідні для навчання матеріали. Доступ до класу слухачі курсу отримують на першому занятті.</p>

Технології навчання	Змішане навчання, проектно-орієнтоване та проблемно-орієнтоване навчання
Політика курсу	<p>Дотримання принципів академічної доброчесності, що визначаються Положенням про запобігання та виявлення плагіату у «Прикарпатський національний університет імені Василя Стефаника»</p> <p>https://pnu.edu.ua/положення-про-запобігання-плагіату/</p> <p>Жодні форми порушення академічної доброчесності не толеруються. Пропущені практичні заняття потрібно виконати і здати з дотриманням процедури захисту роботи.</p> <ul style="list-style-type: none"> самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації» засвоєння пропущеної теми лекції з поважної причини перевіряється під час складання підсумкового контролю. Пропуск лекції з неповажної причини відпрацьовується студентом (співбесіда, реферат тощо). пропущені лабораторні заняття, незалежно від причини пропуску, студент відпрацьовує згідно з графіком консультацій. Поточні „2”, отримані студентом під час засвоєння відповідної теми на практичному, семінарському та лабораторному занятті перескладаються викладачеві, який веде заняття до складання підсумкового контролю з обов'язковою відміткою у журналі обліку роботи академічних груп.

Інформаційні ресурси

Базова література

1. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.
2. Карпенко Станіслав Григорович, Іванов Євген Олександрович Основи інформаційних систем і технологій: Навч. посібник/Міжрегіон. академія управлін. персоналом .-Київ, 2002 .-263с.
3. Новак В.О., Симоненко Ю.Г., Бондар В.П., Матвєєв В.В. Інформаційні системи в менеджменті: Підручник для студ. вищ. навч. закл. К.:Каравела, 2008 .- 615с.
4. Остапов С. Е. Технології захисту інформації : навчальний посібник / С.
5. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 435 с.
6. Грайворонський М.В., Новіков О.М. Безпека інформаційнокомунікаційних систем. – К.: Видавнича група ВНУ, 2009. – 608с.
7. А. В. Жилін, О. М. Шаповал, О. А. Успенський. Технології захисту інформації в інформаційно-телекомунікаційних системах, Навчальний посібник, ІСЗЗІ КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

Допоміжна література

1. Vacca, John R. Network and system security. – Syngress, - 432 p.
2. Грайворонський М. В. Безпека інформаційно-комунікаційних систем /

3. М. В. Грайворонський, О. М. Новіков – К.: Видавнича група ВНУ, 2009. – 608 с.
4. Гребенніков В.В. Історія криптології та секретного зв'язку.
5. Коркішко Т. Алгоритми та процесори симетричного блокового шифрування / Т. Коркішко, А. Мельник, В. Мельник. – Львів. БаК, 2003.
6. Остапов С. Е. Основи криптографії: навчальний посібник / С. Е. Остапов, Л. О. Валь. – Чернівці: Книги–XXI, 2008. – 188 с.

Інформаційні ресурси

Технології захисту інформації - <https://www.uzhnu.edu.ua/uk/infocentre/get/4186>

Захист інформації в комп'ютерних системах та мережах :

http://www.dgma.donetsk.ua/docs/kafedry/avp/metod/_%D0%91%D0%9A%D0%9C%20%D0%9F%D0%BE%D1%81_%D0%B1%D0%BD%D0%B8%D0%BA.pdf

Викладач

Кланічка Ю.В.