МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Кафедра *програмної інженерії та інформаційних технологій управління*
(назва)

«**ЗАТВЕРДЖУЮ**»
Завідувач кафедри
Годлевський М.Д. _____

«_____»_____20_____ року

СІЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ БЕЗПЕКИ ПРОГРАМ ТА ДАНИХ

(назва навчальної дисципліни)

рівень вищої освіти_____*перший (бакалаврський)*_____
перший (бакалаврський) / другий (магістерський)

вид дисципліни _____професійна підготовка (вибіркова)_____
(загальна підготовка (обов'язкова/вибіркова)/ професійна підготовка (обов'язкова/вибіркова))

форма навчання _____денна_____
(денна / заочна)

Харків – 2019 рік

Обсяг дисципліни: __3__ кредитів ECTS _90_ годин.

Лекцій: __16__ годин.

Лабораторних занять: __32__ годин.

Практичних занять: ____ годин.

Форма контролю: іспит.

Термін викладання для освітньо-кваліфікаційного рівня «бакалавр/магістр»: __6__ семестр.

Мова викладання: українська/ англійська.

Мета є навчання студентів принципам побудови комплексних систем захисту інформації, дослідженню та використанню сучасних процедур забезпечення надання основних послуг безпеки інформації в банківських системах, що засновані на використанні алгоритмів симетричної та несиметричної криптографії в комунікаційних системах, протоколів інфраструктури відкритих ключів (ІВК)

Компетентності

Загальні компетентності:

1 Здатність застосовувати знання у практичних ситуаціях.
2 Знання та розуміння предметної області та розуміння професійної діяльності.
3 Здатність вчитися і оволодівати сучасними знаннями.
4 Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Спеціальні (фахові) компетентності:

5 Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки.

Результати навчання. Здатність застосовувати принципи побудови комплексних систем захисту інформації, здатність використання сучасних процедур забезпечення надання основних послуг безпеки інформації в банківських системах, що засновані на використанні алгоритмів симетричної та несиметричної криптографії в комунікаційних системах, протоколів інфраструктури відкритих ключів (ІВК).

Теми, що розглядаються:

Змістовий модуль 1. Принципи безпеки та захисту інформації в ПЗ

Тема 1. Огляд безпеки системи

Тема 2. Механізми і політики розмежування прав доступу.

Тема 3. Методи та пристрої забезпечення захисту і безпеки

Тема 4. Захист, доступ та автентифікація

Тема 5. Моделі захисту.

Тема 6. Шифрування даних

Тема 7. Управління відновленням

Змістовий модуль 2. Інформаційні технології обробки інформації в операційних системах

Тема 8. Основні напрямки розвитку сучасної криптографії

Тема 11. Алгоритми з секретним ключем

Тема 12. Алгоритми з відкритим ключем

Тема 9. Механізми та протоколи керування ключами в ІВК

Тема 13. Протоколи автентифікації

Тема 14. Цифрові підписи

Тема 15. Використання паролів і механізмів контролю за доступом

Форма та методи навчання У курсі використані такі методи навчання: Міні-лекція (викладення навчального матеріалу за короткий проміжок часу й характеризується значною ємністю, складністю логічних побудов, образів, доказів та узагальнень); проблемна лекція (спрямована на розвиток логічного мислення студентів**).**

Методи контролю Оцінювання роботи студентів у процесі лабораторних занять. Проведення проміжного контролю. Проведення модульного контролю.

Розподіл балів, які отримують студенти

Розподіл балів оцінювання успішності студента розраховуються індивідуально для кожної дисципліни з урахуванням особливостей та структури курсу.

Поточна сума балів, що може накопичити студент за семестр може досягати, як максимального балу так і меншого з виділенням балів на іспит чи залік.

В таблиці 1 наведений приклад тих пунктів за якими студент накопичує бали, ці пункти можуть відрізнятися та розглядаються індивідуально для конкретної дисципліни.

Таблиця 1. – Розподіл балів для оцінювання успішності студента

Контрольні роботи	Лабораторні роботи	КР(КП)	РГЗ	Індивідуальні завдання	Тощо	Сума
40	35				25	100

Таблиця 2. – Шкала оцінювання знань та умінь: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
90–100	A	відмінно
82–89	B	добре
74–81	C	
64–73	D	задовільно
60–63	E	
35–59	FX	незадовільно з можливістю повторного складання
0–34	F	незадовільно з обов’язковим повторним вивченням дисципліни

Основна література:

Базова

Євсеєв С.П. Лабораторний практикум з дисципліни “Технології захисту інформації” [Електронний ресурс]. – Режим доступу: ntumoodle.com

1. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.: ил. – Парал. тит. англ.

2. Кузнецов О. О. Захист інформації в інформаційних систе-мах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.

3. Остапов С. Е. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.

4. Хорошко В. А. Методы и средства зашиты информации. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с

Допоміжна література

5. Ленков С.В. Методы и средства защиты информации. В 2-х томах/ С. В. Ленков, Д. А. Перегудов, В. А. Хорошко.– К.: Арий, 2008. – Т.II. Информационная безопасность. – 344 с.

6. Мао Венбо Современная криптография: теория и практика.: Пер. с англ. – М.: Издательский дом “Вильямс”, 2005. – 768 с.

7. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. / А. А. Петров– М.: ДМК, 2000. – 448 с.

8. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник: В 2 т. / В. В. Поповский, А. В. Персиков. – Харьков: ООО “Компания СМИТ”, 2006. – Т.1. – 292 с.

9. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник: В 2 т. / В. В. Поповский, А. В. Персиков. – Харьков: ООО “Компания СМИТ”, 2006. – Т.2. – 252 с.

10. Чмора А.Л. Современная прикладная криптография. / А. Л. Чмора. – М.: Гелиос АРВ, 2001. – 256 с.

Інтернет ресурси

11. http://bezopasnost.biz.

12. http://dstszi.gov.ua.

13. http:// securitylab.ru

14. http:// pgpi.org

15. http:// citmgu.ru

Структурно-логічна схема вивчення навчальної дисципліни

Таблиця 3. – Перелік дисциплін

Вивчення цієї дисципліни безпосередньо спирається на:	На результати вивчення цієї дисципліни безпосередньо спираються:
“Вища математика”	
“Математичне програмування”	
“Інформатика та комп’ютерна техніка”	

Провідний лектор: проф. Євсеєв С.П. _____