**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**
**«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»**

**Навчально-науковий інститут інформаційних технологій і механотроніки**
**Кафедра комп'ютерних та інформаційних технологій і систем**

# СИЛАБУС

# НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

# «ЗАХИСТ ІНФОРМАЦІЇ»

**141БВБ.8.2**

| | | |
|---|---|---|
| Освітній рівень | Перший (бакалавр) | |
| Програма навчання | обов'язкова | |
| Галузь знань | 14 | Електрична інженерія |
| Спеціальність | 141 | Електроенергетика, електротехніка та електромеханіка |
| Освітня програма | Електромеханічні системи автоматизації та електропривод | |
| Обсяг дисципліни | 6 кредити (180 академічних годин) | |
| Види аудиторних занять | Лекції (18 академічних годин), практичні заняття (12 академічних годин), лабораторні заняття (10 академічних годин) | |
| Графік вивчення дисципліни | четвертий рік, осінній семестр | |
| Індивідуальна робота | Індивідуальне завдання – ргр | |
| Форма контролю | екзамен | |

**Координатор курсу: Головко Г.В. доцент кафедри Комп'ютерних та інформаційних технологій і систем, к.т.н., доцент**

**https://nupp.edu.ua/page/sklad-kafedri-kompyuternikh-ta-informatsiynikh-tekhnologiy-i-sistem.html**

**(понад 90 публікацій наукового, науково-методичного і науково-технічного характеру, з поміж яких 1 у НБД Web on Science, понад 60 статей у фахових виданнях)**

**Асистент координатора: Головко Г.В. доцент кафедри Компютерних та інформаційних технологій і систем, к.т.н., доцент**

**https://nupp.edu.ua/page/sklad-kafedri-kompyuternikh-ta-informatsiynikh-tekhnologiy-i-sistem.html**

**Мета**: навчити студентів правильно проводити аналіз погроз безпеці інформації, організовувати політику безпеки згідно світовим стандартам, закласти математичний та термінологічний фундамент в галузі криптології, основним методам, механізмам, алгоритмам та протоколам криптографічного захисту інформації в інформаційно – комунікаційних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз та проведення криптографічного аналізу зі сторони потенційних порушників.

**Завдання:** У цьому курсі передбачається формування у студентів певних професійних компетенцій, знань та вмінь з теорії та практики організації політику безпеки, криптографічного захисту інформації та криптографічного аналізу.

У результаті вивчення навчальної дисципліни студент повинен
**знати:**

- канали уразливості та витоку інформації, явища, що притаманні їх прояву та існуванню;
- основні методи, механізми, протоколи та алгоритми криптографічного захисту інформації;
- критерії та показники оцінки якості криптографічного захисту інформації;
- методи криптографічних перетворень інформації та способи їх здійснення;
- методи та засоби аналізу та крипто аналізу асиметричних та симетричних крипто перетворень;
- основні протиріччя, проблеми, тенденції та напрями розвитку теорії та практики криптографічного захисту інформації, прогнозування їх можливостей та можливостей порушників(крипто аналітиків);
- функціональні можливості та порядок застосування сучасних пакетів програмної реалізації криптографічних перетворень та криптографічних бібліотек.

**вміти:**

розробляти політику безпеки згідно світовим стандартам, проводити аналіз погроз безпеці інформації та володіти основними методами, механізмами, алгоритмами захисту інформації в інформаційно – комунікаційних системах з урахуванням сучасного стану та прогнозу здійснення погроз

обґрунтовувати, вибирати та застосовувати критерії та показники оцінки стійкості криптографічних перетворень та безпечності криптографічних протоколів;

розробляти вимоги та обирати для застосування криптографічні перетворення та протоколи, що мінімізують впливи порушників;

розробляти моделі загроз безпеці інформації, вирішувати завдання аналізу та синтезу криптографічних алгоритмів та протоколів захисту інформації.

**Компетентності за ОПП:**

**ЗК01.** Здатність до абстрактного мислення, аналізу та синтезу.
**ЗК02.** Здатність застосовувати знання у практичних ситуаціях.
**ЗК05.** Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
**ЗК06.** Здатність виявляти, ставити та вирішувати проблеми.
**ЗК07.** Здатність працювати в команді.
**ЗК08.** Здатність працювати автономно.
**СК14.** Здатність вирішувати комплексні спеціалізовані задачі і практичні проблеми, пов’язані з проблемами метрології, електричних вимірювань, роботою пристроїв автоматичного керування, релейного захисту та автоматики.

**Програмні результати навчання за ОПП:**

**ПР02.** Знати і розуміти теоретичні основи метрології та електричних вимірювань, принципи роботи пристроїв автоматичного керування, релейного захисту та автоматики, мати навички здійснення відповідних вимірювань і використання зазначених пристроїв для вирішення професійних завдань.
**ПР06.** Застосовувати прикладне програмне забезпечення, мікроконтролери та мікропроцесорну техніку для вирішення практичних проблем у професійній діяльності.
**ПР10.** Знаходити необхідну інформацію в науково-технічній літературі, базах даних та інших джерелах інформації, оцінювати її релевантність та достовірність.

**Структура навчальної дисципліни**

| Назви змістових модулів і тем Назви змістових модулів і тем | Кількість годин | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | денна форма | | | | | | Заочна форма | | | | | |
| | усього | у тому числі | | | | | усього | у тому числі | | | | |
| | | л | п | лаб | інд | с.р. | | л | п | лаб | інд | с.р. |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| **Змістовий модуль 1. Поняття інформаційної безпеки і її місце в системі національної безпеки.** | | | | | | | | | | | | |
| **Тема 1** Види і джерела погроз ІБ. Система нормативно-правових актів, що регламентують забезпечення ІБ**.** Види інформації. Основні поняття захисту інформації (об'єкти, суб'єкти, канали витоку, НСД, рівні доступу(СІ і СОП). Протиправна діяльність в інформаційній сфері | 32 | 4 | 8 | | 6 | 14 | | | | | | |
| **Тема 2** Модель Белла-Лападули, як основа побудови систем мандатного розмежування доступу. Основні положення моделі. Основна теорема безпеки.. Види і джерела погроз ІБ: а) дискреційна політика безпеки; б) мандатна політика безпеки. | 32 | 4 | 8 | | 6 | 14 | | | | | | |
| **Тема** 3. Бази даних, класифікація баз даних, поняття цілісності і несуперечності бази даних, методи і засоби забезпечення цілісності і несуперечності. Поняття банку даних, властивості банку даних: незалежність, обмеженість доступу стосовно яких параметрів/крапкам (об'єктам) банку даних можна обмежити доступ, як це реалізується, які | 26 | 4 | 8 | | 4 | 10 | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| недоліки вони усувають | | | | | | | | | | | | |
| **Разом за змістовим модулем 1** | **90** | **12** | **24** | | **16** | **38** | | | | | | |
| **Змістовий модуль 2 Організація захисту інформації** | | | | | | | | | | | | |
| | | | | | | | 12 | | | | | |
| **Тема 4.** Особливості організації захисту від різних видів шкідливого програмного забезпечення..Файлово-серверна і клієнт-серверна архітектури: опис, достоїнства і недоліки системи з колективним використанням файлів, системи з архітектурою клієнт-сервер: організація, достоїнства і недоліки. | 44 | 6 | 8 | | 14 | 16 | | | | | | |
| **Тема 5.** Основні поняття криптографії. Стійкість шифрів. Теоретична і практична стійкість криптосистем. Узагальнена схема для криптосистем із закритими ключами шифрування. Основні історичні етапи становлення криптографії. Криптографічні і стеганографічні методи захисту інформації | 46 | 6 | 8 | | 16 | 16 | | | | | | |
| **Разом за змістовим модулем 2** | **90** | **12** | **16** | | **30** | **32** | | | | | | |
| **Усього годин** | **180** | **24** | **40** | | **46** | **66** | | | | | | |

## 5 Теми семінарських занять

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| | Семінарські заняття не передбачені | |

## 6 Теми практичних занять

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1. | Основні поняття захисту інформації<br>Система нормативно-правових актів, що регламентують забезпечення ІБ. Види інформації. | 8 |

| | | |
|---|---|---|
| 2 | Основа побудови систем мандатного розмежування доступу. Модель Белла-Лападули як основа побудови систем мандатного розмежування доступу. і | 8 |
| 3. | Облікові записи користувачів і груп, збереження інформації | 8 |
| 4. | Особливості організації захисту від різних видів шкідливих програмних продуктів. | 6 |
| 5.. | Основні поняття криптографії. Стійкість шифрів. Теоретична і практична стійкість криптосистем. | 6 |
| | ***Разом*** | 40 |

**7. Теми лабораторних занять**

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| | Лабораторні заняття не передбачені | |
| | | |

**8. Самостійна робота**

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Протиправна діяльність в інформаційній сфері.<br>Карно-процесуальна характеристика комп'ютерних злочинів.<br>Основні задачі організаційної системи забезпечення ІБ.<br>яття політики забезпечення ІБ | 14 |
| 2 | Збереження інформації про облікові записи на твердому диску, класична атака по скиданню і підборові пароля користувача, способи захисту система, реалізація,методи збереження інформації про дискові блоки, що належать файлові в FAT, Ext2, NTFS, засобу забезпечення надійності і високої продуктивності ФС | 14 |
| 3 | Облікові записи користувачів і груп, збереження інформації про облікові записи на твердому диску, класична атака по скиданню і підборові пароля користувача, способи захисту система, реалізація,методи збереження інформації про дискові блоки, що належать файлові в FAT, Ext2, NTFS, засобу забезпечення надійності і високої продуктивності ФС. | 10 |
| 4 | Основні історичні етапи становлення криптографії. Криптографічні і стеганографічні методи захисту інформації | 32 |
| | **Разом** | **66** |

**9. Індивідуальні завдання**

Метою індивідуальних завдань, що враховують навчальні потреби та можливості кожного конкретного студента, є систематизація, узагальнення, закріплення та розширення теоретичних знань, котрі студенти одержують у процесі навчання, а також застосування цих знань на практиці. Такі завдання створюють умови для якнайповнішої реалізації творчих можливостей тих студентів, які виявили особливі здібності в навчанні та нахил до науково-дослідної роботи й творчої діяльності. Індивідуальні завдання виконуються студентами самостійно під керівництвом викладачів.

Види індивідуальної роботи студента:

- виконання індивідуальних навчально-дослідних завдань (написання рефератів для участі у конкурсі рефератів, розробка й виготовлення ілюстративних схем, порівняльних таблиць, пошук і добирання інформації з певної теми, зокрема з Інтернету);
- виконання доручень науково-дослідницького характеру (підготовка доповіді на студентську або загальноуніверситетську наукову конференцію, написання наукової статті або тез

виступу, підготовка й участь у конкурсі студентських наукових робіт).

Загальний обсяг часу на індивідуальну роботу складає 20 год.

За власним бажанням та вибором студента додатково, з метою отримання додаткових «призових» балів, він може виконати реферат на одну із тем, поданих у наступному переліку, або запропонувати та погодити з викладачем власну тему.

При виконанні роботи студент спирається на: Методичні рекомендації для самостійної роботи студентів з дисципліни «Захист інформації» напряму підготовки 6.050101 «Комп'ютерні науки», всіх спеціальностей та всіх форм навчання. / Полтава: ПолТНТУ, 2013. – 202 с

.**Перелік тем для рефератів:**

1. Захист інформації на носіях
2. Інформаційна безпека систем керування базами даних
3. Ідентифікація та аутентифікація користувача
4. Безпека електронних платіжних систем
5. Організація захисту інформації в мережному середовищі розподілених відомчих інформаційно-обчислювальних систем
6. Комп'ютерні атаки і технології їхнього виявлення
7. Аналіз захищеності баз даних
8. .Порівняльна характеристика файлових систем FAT32 та NTFS.
9. Захист електронних документів
10. Захист електронних таблиць
11. Захист баз даних
12. Захист протоколів мережі
13. Види симетричних шифрів.
14. Алгоритм асиметричних шифрів
15. Електронний цифровий підпис.
16. " Небезпечні програми"
17. Принцип роботи криптосистеми
18. Перспективи розвитку інформаційної безпеки

## 10. Методи навчання

При викладанні дисципліни застосовуються словесні, наочні та практичні методи навчання.

Словесні і наочні використовуються під час лекцій та інструктажів, практичні при проведенні практичних занять.

Під час проведення лекцій використовуються такі словесні методи як розповідь, пояснення та наочні методи: ілюстрація, демонстрація.

Перед проведенням практичних занять викладачами проводяться інструктажі: вступні, поточні, підсумкові.

Під час проведення практичних занять застосовуються наочні спостереження та словесні бесіди: вступні, поточні, репродуктивні, евристичні, підсумкові; студентами виконуються вправи: тренувальні, творчі, усні, практичні, технічні.

## 11. Методи контролю

Способами контролю знань студентів є такі:

– опитування й оцінювання знань студентів під час лабораторних занять;

– оцінювання виконання студентами на практичному занятті індивідуальних завдань;

– перевірка конспектів лекцій і лабораторних робіт;

– проведення і перевірка письмових контрольних робіт, поточного тестування на лабораторних заняттях;

– модульний контроль (проміжний);

– індивідуальні співбесіди;

– підсумковий контроль (екзамен).

**Поточний контроль** успішності засвоєннями студентами навчального матеріалу здійснюється під час проведення лабораторних занять і має на мету перевірку рівня підготовленості студента до виконання конкретної роботи. Вибір конкретних форм і методів поточного контролю знань студентів залежить від викладача і доводиться до їхнього відома на першому занятті.

**Модульний контроль** проводиться наприкінці кожного змістового модуля за рахунок аудиторних занять і має на меті перевірку засвоєння студентом певної сукупності знань та вмінь, що формує цей модуль. Модульний контроль реалізується шляхом узагальнення результатів поточного контролю знань і проведення спеціальних контрольних заходів (у формі тестування чи написання студентами контрольних робіт), проводиться наприкінці кожного змістового модулю за рахунок аудиторних занять, під час групових консультацій або ж за рахунок часу, відведеного на самостійну роботу студентів. На підставі результатів модульного контролю здійснюється міжсесійний контроль (атестація)..

| **№ та назва змістового модуля** | **Форма контролю** | **Час проведення** |
|---|---|---|
| **Змістовий модуль 1.** Поняття інформаційної безпеки та її місце в системі національної безпеки. | Тестування | Практичне заняття № 3 |
| **Змістовий модуль 2.** Організація захисту інформації**.** | Тестування | Практичне заняття № 5 |

**Підсумковий контроль** –, екзамен, проводиться в формі тестування під час екзаменаційної сесії за умови виконання графіку навчального процесу при наявності рейтингової оцінки за теоретичний курс 30 і більше балів.

## 12. РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ (ДЕННОЇ ФОРМИ НАВЧАННЯ)

| Поточне тестування та самостійна робота | Підсумковий контроль екзамен | Сума |
|---|---|---|
| | 50 | 100 |

**Шкала оцінювання: національна та ECTS**

| Сума балів за всі види навчальної діяльності | Оцінка ECTS | Оцінка за національною шкалою |
|---|---|---|
| | | для екзамену, диференційованого заліку, курсового проекту (роботи), практики |
| 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 |

## 13. Методичне забезпечення

1. Конспект лекцій.
2. Методичні вказівки до лабораторних робіт.
3. Методичні вказівки для виконання індивідуальних завдань.
4. Методичні рекомендації з виконання розрахунково-графічної роботи.

.5. Правила модульно-рейтингового оцінювання знань із навчальної дисципліни.

## 14. Рекомендована література

### Базова


1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний підручник. Харків, ХНУРЕ, 2011 р.
2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. Харків, ХНУРЕ, 2011 р.
3. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.
4. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2010 , 593с.
5. Есин В. И., Кузнецов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.


### Допоміжна


6. Задірака В. Компьютерная криптологія. Підручник. К, 2002 ,504с.
7. Бембо Мао. Современная криптографія. Теорія и практика. Москва. 2005.
8. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Изд. Триумф. М., 2003 г. 815 с.
9. Б. Шнайер . Безопасность данных в цифровом мире. Изд. Питер. Харьков. 2003 г. 367 с.
10. В. Столлингс. Криптография и защита сетей. Принципы и практика. Изд. “Вильямс”. К. 2001. 669 с.
11. Шеннон К. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333-369 ( Також «Введение в криптографию» под ред. В. В. Ященко // http://nature.web.ru/db/msg.html?mid=1157083&uri=node1.html).
12. А. Менезис, П. Ван Аршот, С. Ватсон. Руководство по прикладной криптографии CRC Press, 1997, электронная копия, 662 с.


.

## 15. Інформаційні ресурси

Закон України від 15 грудня 2005 року № 3200-IV "Про основи національної безпеки України".

Закон України "Про інформацію". Із змінами, внесеними згідно із Законом від 07.02.2002 № 3047-III-ВР.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 № 2594-IV.

Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IX.