МІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ АВТОМОБІЛЬНО-ДОРОЖНІЙ УНІ-ВЕРСИТЕТ

Кафедра комп'ютерних технологій і мехатроніки

«ЗАТВЕРДЖУЮ»
Гарант освітньо-професійної програми «Програмне забезпечення систем» першого (бакалаврського) рівня вищої освіти, завідувач кафедри КТМ, д.т.н.,
професор _____ **Ніконов О.Я.**
«03» 09 **2019р.**

СИЛАБУС
ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ//
CYBERSECURITY INFORMATION TECHNOLOGY
SYLLABUS

освітній ступінь	**бакалавр** / bachelor
галузь знань	**12 Інформаційні технології /** Information Technology
спеціальність	**121 Інженерія програмного забезпечення /** Software Engineering
освітня програма	**Програмне забезпечення систем /** Systems Software

Харків 2019

Автор: Мнушка Оксана Василівна, асистент кафедри комп’ютерних технологій і мехатроніки

Силабус розглянуто та затверджено на засіданні кафедри комп’ютерних технологій і мехатроніки, протокол № 18 від «27» червня 2019 р.

СИЛАБУС

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ /

CYBERSECURITY INFORMATION TECHNOLOGY

SYLLABUS

освітній ступінь	**бакалавр** / bachelor
галузь знань	**12 Інформаційні технології /** Information Technology
спеціальність	**121 Інженерія програмного забезпечення /** Software Engineering
освітня програма	**Програмне забезпечення систем /** Systems Software

Анотація курсу

1. **Викладачі**

1.1. Лектор: Мнушка Оксана Василівна

- асистент кафедри комп'ютерних технологій та мехатроніки;
- педагогічний стаж – 16 років
- контактний телефон +38-057-707-37-43
- e-mail: mnushka.ov@gmail.com
- наукові інтереси: комп'ютерні мережі, інформаційні технології керування, безпека даних, групові комунікації.

1.2. Асистент лектора:

2. **Дисципліна** «Технології захисту інформації»

- рік навчання: 3;
- семестр навчання: 5;
- кількість годин за семестр: 120, в т. ч.
  лекційних: 16;
  практичних занять: 32;
  на самостійне опрацювання: 72;
- кількість аудиторних годин на тиждень
  лекційних: 2 (раз на два тижні);
  практичних занять: 2.

3. **Час та місце проведення**

- аудиторні заняття – відповідно до розкладу ХНАДУ, ауд. 214, 216;
- позааудиторна робота – самостійна робота студента із використанням технологій віртуалізації Oracle, хмарних технологій Google та Microsoft.

4. **Пререквізити та постреквізити навчальної дисципліни:**

- **пререквізити**: «Операційні системи», «Алгоритмізація та програмування», «Мережні технології та системне адміністрування», «Дискретна математика», «Об’єктно-орієнтоване програмування»
- **постреквізити (**дисципліни та компетентності, які необхідні в професійній діяльності фахівця**)**: «Професійна практика програмної інженерії», «Геоінформаційні системи». Software Engineer, Software Architect

5. Характеристика дисципліни:

5.1. Призначення навчальної дисципліни: основу дисципліни «Технології захисту інформації» становить вивчення основних положень та принципів побудови та використання програмних та апаратно-програмних засобів забезпечення безпеки програм та даних у комп’ютерних системах та мережах. Опанування сучасних технологій роботи із даними на рівні створення та налагодження програмного забезпечення, засвоєння та використання методів захисту даних та програмного забезпечення є необхідним компонентом підготовки кваліфікованого інженера-програміста (Software Engineer), системного архітектора (System Architect), архітектора програмного забезпечення (Software Architect).

5.2. Мета вивчення дисципліни: отримання теоретичних знань про методи кодування, шифрування та захисту інформації; типові загрози методи боротьби із ними; особливості проектування, програмування та налаштування контролів захисту для програмних систем та даних, що у них зберігаються для безперебійного та ефективного використання комп’ютерних технологій

5.3. Задачі вивчення дисципліни:

- основні загрози для цілісності даних;
- типи атак на програмне забезпечення;
- методи шифрування даних;
- методи кодування даних;
- методи криптографічного захисту даних;
- коригуючі коди;
- стеганографічні методи захисту даних;
- методи крипто- та стеганоаналізу;
- програмне забезпечення для кодування та шифрування даних;

– засоби операційних систем для захисту даних та програм;
– апаратні та апаратно-програмні рішення для захисту даних
–

5.4. Зміст навчальної дисципліни: відповідає навчальній та робочій програмі, які відповідають вимогам до відповідних фахівців на ринку праці.

5.5. План вивчення дисципліни:

Результати навчання	**Навчальна діяльність**	**Робочий час студента (год.)**	**Оцінювання (бал)**
Знати: - основні поняття про загрози для даних в комп'ютерних системах; - міри вимірювання інформації; - визначення даних, інформації, коду; - поняття про похибки та методи їх корегування.	**Тема 1.** Вступ. Основи теорії кодування даних. Кодування мультимедійних даних **Лекція 1.** План лекції. 1. Мета та задачі вивчення дисципліни 2. Загрози для цілісності даних та програм 3. Дані, інформація, коди 4. Коди та кодування даних 5. Коригуючі коди. **Список рекомендованих джерел** Основний 1-8 Додатковий 1-5	2	
Вміти: - визначити параметри повідомлення; - будувати алгоритм для методів кодування.	**Самостійна робота студентів**: – інформація, міри інформації; – коди.	5	4
Вміти: - реалізовувати відповідні алгоритми для роботи із коригуючими кодами на обраній мові програмування	**Практична робота 1.** Коригуючі коди. Задання на практичну роботу: написати програму для дослідження роботи коригуючих кодів: – Гемінга; – CRC16; – CRC32. План заняття: – актуалізація теоретичного матеріалу; – виконання завдань; – презентація результатів роботи.	4	8

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
Знати: - типи кодів - структуру коду Шеннона-Фано - структуру коду Хаффмена - методи ефективного кодування	**Тема 2.** Поширені методи ефективного кодування даних для комп'ютерних систем загального призначення **Лекція 2.** План лекції. 1. Типи кодів 2. Поняття про ефективне кодування 3. Код Шеннона-Фано 4. Код Хаффмена **Список рекомендованих джерел** Основний 1-8 Додатковий 1-5	2	1
Вміти: - описувати методи та алгоритми стиснення даних; - розрізняти методи із втратами та без втрат інформації	**Самостійна робота студентів** – методи стиснення даних; – алгоритм Лемпеля-Зіва-Велча.	5	3
Вміти: - реалізовувати заданий алгоритм на обраній мові програмування	**Практична робота 2.** Метод Лемпеля-Зіва. Задання на практичну роботу: написати програму для дослідження роботи методів кодування згідно варіанту: – код Шеннона-Фано; – код Хаффмена; – алгоритм Лемпеля-Зіва-Велча. План заняття: – актуалізація теоретичного матеріалу; – виконання завдань; – презентація результатів роботи.	4	8
Знати: - класичні методи шифрування - методи оцінки стійкості шифрів	**Тема 3.** Методи криптографічного захисту даних. Шифри та їх використання. **Лекція 3.** План лекції. 1. Розвиток методів шифрування 2. Підстановка 3. Перестановка 4. Гамування **Список рекомендованих джерел** Основний 1-8 Додатковий 1-5	2	1
Вміти:	**Самостійна робота студентів**	6	3

Результати навчання	**Навчальна діяльність**	**Робочий час студента (год.)**	**Оцінювання (бал)**
- розробляти алгоритм до заданого методу шифрування - вміти обирати метод шифрування для заданої задачі	– класичні методи а алгоритми шифрування даних; – сучасні методи а алгоритми шифрування даних.		
Вміти: - реалізовувати заданий метод шифрування на обраній мові програмування	**Практична робота 3.** Методи шифрування даних Задання на практичну роботу: написати програму для дослідження роботи методів кодування згідно варіанту: – підстановка; – перестановка; – гамування. План заняття: – актуалізація теоретичного матеріалу; – виконання завдань; – презентація результатів роботи.	4	8
Знати: - методи симетричного шифрування - методи несиметричного шифрування	**Тема 4.** Методи шифрування даних у комп'ютерних системах загального призначення, симетричні та асиметричні схеми шифрування. **Лекція 4.** План лекції. 1. Сучасні підходи до шифрування даних 2. Симетричні методи шифрування та блочні коди 3. Асиметричні методи шифрування та шифри **Список рекомендованих джерел** Основний 1-8 Додатковий 1-5	2	1
Вміти: - визначати параметри шифрів; - вибрити метод шифрування для заданої задачі; - аналізувати криптостійкість алгоритмів.	**Самостійна робота студентів:** – стандарти шифрування даних; – крипостійкість алгоритмів.	5	4

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
Вміти: - реалізовувати заданий метод шифрування на обраній мові програмування; - використовувати стандартні криптографічні бібліотеки для створення програми; - обирати алгоритм в залежності від специфіки задачі.	**Практична робота 4.** Дослідження криптостійкості блочних симетричних кодів. Завдання на практичну роботу: реалізувати та дослідити роботу алгоритму згідно варіанту – алгоритм RSA; – алгоритм DES. План заняття: – актуалізація теоретичного матеріалу; – виконання завдань; – презентація результатів роботи.	4	8
Знати: - класифікацію загроз для програм та даних; - політики розмежування прав доступу; - методи побудови хеш-функцій; - методи шифрування паролів	**Тема 5.** . Безпека програм та даних на основі механізмів та політик розмежування прав доступу до даних. **Лекція 5.** План лекції. 1. Типові загроза даним під час виконання програм 2. Поняття про політики розмежування 3. Розмежування доступу у різних операційних системах 4. Хеш-функції 5. Оцінювання стійкості паролів та хеш-функцій **Список рекомендованих джерел** Основний 1-11 Додатковий 1-9	2	1
Вміти: - використовувати політики безпеки на локальному комп’ютері - Використовувати програмне забезпечення для аудиту безпеки - Використовувати антивірусне	**Самостійна робота студентів:** – політики безпеки на локальному комп’ютері; – політики безпеки у домені підприємства (організації)	5	4

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
та антишпигунське програмне забезпечення			
Вміти: - використовувати стандартні бібліотеки для розробки програм та реалізації заданого методу; - реалізовувати алгоритми побудови хеш-функцій	**Практична робота 5.** Використання хеш-сум для захисту даних. Завдання на практичну роботу: написати програму для – оцінювання використання хеш-функцій (на прикладі MD5); – оцінювання стійкості паролю до зламу. План заняття: – актуалізація теоретичного матеріалу; – виконання завдань; – презентація результатів роботи.	4	8
Знати: - методи приховування даних у мультимедійних потоках; - методи побудови стеганографічних зображень; - оцінки стійкості обраних методів.	**Тема 6.** Методи захисту даних та програм на основі алгоритмів приховування інформації в потоках даних **Лекція 6.** План лекції. 1. Захист даних на основі приховування інформації 2. Стеганографічні методи захисту даних **Список рекомендованих джерел** Основний 1-11 Додатковий 1-9	2	1
Вміти: - використовувати стандартне програмне забезпечення для побудови стеганографічних зображень	**Самостійна робота студентів** – стеганографія; – утиліти для кодування/декодування.	5	4
Вміти: - використовувати стандартне програмне забезпечення для побудови та аналізу стеганографічних зображень.	**Практична робота 6.** Методи приховування інформації в потоках даних. Завдання на практичну роботу: 1. Дослідити роботу алгоритмів приховування даних у зображенні. 2. Дослідити стійкість стеганографічних методів захисту інформації. План заняття: – актуалізація теоретичного матеріалу;	4	8

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
	– виконання завдань; – презентація результатів роботи		
Знати: - основні загрози для програм, що виконуються; - методи захисту даних в програмах; - методи захисту коду програми	**Тема 7.** Методи захисту програм та даних під час виконання, захист носіїв даних.. **Лекція 3.** План лекції. 1. Захист даних в мережі 2. Захист даних в програмах, що виконуються 3. Захист програмного коду від налагодження **Список рекомендованих джерел** Основний 1-11 Додатковий 1-6	2	1
Вміти: - використовувати спеціальне програмне забезпечення для захисту коду програми	**Самостійна робота студентів** Апаратні та програмні засоби захисту програм та даних	5	2
Вміти: - використовувати спеціальне програмне забезпечення для захисту коду програми; - використовувати утиліти для аналізу коду програм, що виконуються.	**Практична робота 7.** Методи захисту виконуваних файлів (програм) від зламу та налагодження Завдання на практичну роботу: дослідити роботу утиліт для захисту програм, що виконуються - налагодження та його використання для аналізу коду програми, утиліти для налагодження; - утиліти для захисту програм від налагодження та аналізу. План заняття: – актуалізація теоретичного матеріалу; – виконання завдань; – презентація результатів роботи.	4	8
Знати: апаратні методи автентифікації та ідентифікації; - біометричні методи автентифікації та ідентифікації;	**Тема 8.** Сучасні методи автентифікації та ідентифікації користувачів для захисту даних – цифровий підпис, біометричні методи автентифікації. **Лекція 3.** План лекції. 1. Цифровий підпис 2. Біометрична ідентифікація	2	1

Результати навчання	**Навчальна діяльність**	**Робочий час студента (год.)**	**Оцінювання (бал)**
- методи побудов електронних цифрових підписів; - методи цифрових підписів електронних документів.	3. Автентифікація на основі цифрових технологій 4. Автентифікація на основі біометричних даних. **Список рекомендованих джерел** Основний 1-11 Додатковий 1-9		
Вміти: - обирати метод ідентифікації та автентифікації в залежності від специфіки задачі.	**Самостійна робота студентів:** - біометричні методи ідентифікації; - біометричні методи автентифікації; - проблеми використання біометричних методів ідентифікації та автентифікації;	6	4
Вміти: - використовувати GnuPG для цифрового підпису документів.	**Практична робота 8.** Електронний цифровий підпис документів. 1. Дослідити роботу систем для підпису документів на прикладі GnuPG. 2. Створення сертифікатів, створення облікового запису, створення підпису. 3. Захист документів та електронної пошти за допомогою цифрових підписів План заняття: – актуалізація теоретичного матеріалу; – виконання завдань; – презентація результатів роботи	4	8
Вміти: - використовувати вивчені методи та алгоритми для розв’язання прикладних задач.	**Самостійна робота студентів:** підготовка до складання іспиту	30	1
Разом		**120** *годин/* **4** *кредити*	**100** *балів*
Підсумковий контроль		письмовий екзамен	

6. Список рекомендованих джерел:

6.1.Основний:

1. Технології захисту інформації : навч. посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2013. – 476 с.

2. Жураковский Ю.П., Полторак В.П. Теорія інформації кодування: Підручник. - Київ : Вища школа, 2001. - 255 с.

3. Теорія інформації та кодування : навч. посібник / В.Л. Кожевников, А.В. Кожевников. – Дніпродзержинськ : Національний гірничий університет, 2012. – 108 с.

4. Захист інформації в автоматизованих системах управління : навч. посібник / Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

5. Основы стеганографии. / А.В. Аграновский, П.Н. Девянин, А.В. Черемушкин, Р.А. Хади. – Ростов на Дону, 2003. – 117 с.

6. Основы криптографии. / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – Гелиос АРВ, 2002. – 480 с.

7. Белоногов В. А. Теория кодирования: учебное пособие. / В.А. Белоногов. – Екатеринбург : УГТУ-УПИ, 2002 . – 111 с.

8. Бородин Л.Ф. Введение в теорию помехоустойчивого кодирования. / П.Ф. Бородин. – М.: Советское радио, 1968. – 407 с.

9. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. / В.Е. Козлов. – Горячая линия – Телеком, 2002. – 336 с.

10. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. – Київ: Арий, 2008. – Том I. Несанкционированное получение информации. – 464 с..

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

6.2. Додатковий:

1. Літнарович Р.М. Сучасні технології інформаційної безпеки. Част. 1. Навчальний посібник. – МЕГУ, Рівне, 2011. – 97 с.

2. Шеннон К.Э. Теория связи в секретных системах. / К.Э. Шеннон //Шеннон К.Э. Работы по теории информации и кибернетике. – М.: ИЛ, 1963. – С. 333–402.

3. В.А. Хорошко. Методы и средства защиты информации. / В.А. Хорошко, А.А. Чекотков. – К.: Юніор, 2003. - 479 с.

4. Столингс В. Криптография и защита сетей: принципы и практика. 3-е изд. /М: Издательский дом «Вильямс», 2001. – 672 с.

5. В.В. Домарев. Безопасность информационных технологий. Методология создания систем защиты. — К.: ООО “ДС”, 2005. - 688 с.

6. Цымбал В.П. Задачник по теории информации и кодирования. - Киев: Издательское объединение “Вища школа”, 2000. – 268 с.

7. Лигун А.О., Комп’ютерна графіка (Обробка та стиск зображень) / А.О.Лигун, О.О.Шумейко . – Дніпропетровськ: Біла К.О., 2010 . – 114 с.

8. Романец Ю.В Защита информации в компьютерных сетях. / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин . – М.: Радио и связь, 2001. – 376 с.

9. Фленов М.Е.Web-сервер глазами хакера/М.Е.Фленов . –BHV-СПб,2009 . – 320 с.

6.3. Інформаційні ресурси:

1. Захист інформації – [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Захист_інформації.

2. Комплексні системи захисту інформації /[Електронний ресурс]. [Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін]– Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/

3. Технології захисту інформації [Електронний ресурс, URL: http://umm.pstu.edu/handle/123456789/7947] : методичні вказівки до самостійного вивчення дисципліни «Технології захисту інформації» для студентів напряму підготовки 6.050101 «Комп'ютерні науки» всіх форм навчання / уклад. С. В. Альошин. – Маріуполь : ПДТУ, 2015. – 37 с.

4. Ахрамович В. М. Навчальна програма дисципліни «Технології захисту інформації» (для спеціалістів) [Електронний ресурс, URL: http://library.iapm.edu.ua/metod_disc/pdf/4086up.pdf]. – К.: ДП «Вид. дім «Персонал», 2012. – 16 с.

5. Єгоров А.О. Методичні вказівки до виконання лабораторних робіт з дисципліни «Технології захисту інформації» [Текст], [Електронний ресурс, URL: http://repository.dnu.dp.ua:1100/upload] / А.О. Єгоров, Н.О. Соколова – Д.: НМетАУ, 2014. – 85 с.

7. Контроль та оцінювання результатів навчання: положення про оцінювання результатів навчання студентів і аспірантів наказ ХНАДУ №__ від __._____ 20__ р. Під час вивчення дисципліни «Безпека програм та даних» викладачем здійснюється поточний та підсумковий контроль. Поточний контроль та оцінювання передбачає:

- перевірку рівня засвоєння теоретичного матеріалу (тестування за матеріалами лекції, який здійснюється на початку кожної наступної лекції);
- захист практичних робіт (проходить під час наступної практичної роботи);

8. Політика навчальної дисципліни:

8.1. Відвідування лекційних та практичних занять: відвідування лекційних та практичних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попереднього домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).

8.2. Відпрацювання пропущених занять: відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має були відпрацьоване до наступної лекції на консультації викладача. Від-

працювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Практичне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті університету).

8.3. Правила поведінки під час занять: обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчального матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем).

8.4. За порушення академічної доброчесності студенти будуть притягнені до академічної відповідальності у відповідності до положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти ХНАДУ (Наказ ХНАДУ від __._____.20__ №____).

Студенти будут притягнені до такої академічної відповідальності:

- Повторне проходження оцінювання (контрольна робота, іспит, залік тощо);
- Повторне проходження навчального курсу.