**Форма ХНАДУ**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний автомобільно-дорожній університет

Група _МП-31_

**ЗАТВЕРДЖУЮ**
Перший проректор з НПР
професор _____ С.Я. Ходирєв
"31" 09 2020 року

# РОБОЧА ПРОГРАМА

**навчальної дисципліни** _____Безпека програм і даних_____
(назва навчальної дисципліни згідно освітньої програми)

**підготовки** _____бакалавра_____
(назва освітньо-кваліфікаційного рівня)

**в галузі знань** _____12 Інформаційні технології_____
(шифр і назва галузі знань)

**спеціальності** __121 Інженерія програмного забезпечення_____
(шифр і назва спеціальності)

**за освітньою програмою**[1] _Програмне забезпечення систем _
(назва освітньо-професійної (освітньо-наукової) програми)

**мова навчання** _____державна_____
(мова, на якій проводиться навчання за робочою програмою)

2020 рік

[1] *якщо програма навчальної дисципліни розроблена для декількох освітніх програм за даною спеціальністю, то вказуються усі освітні програми*

**1. Мета вивчення навчальної дисципліни** є 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.

**2. Передумови для вивчення дисципліни**: основи інформаційних технологій, алгоритмізація та програмування, дискретна математика, окремі розділи вищої математики.

**3. Опис навчальної дисципліни**

| Найменування показників | Характеристика навчальної дисципліни[2] | |
|---|---|---|
| | **денна форма навчання** | **заочна (дистанційна) форма навчання**[3] |
| **Кількість кредитів** - __4__<br>**Кількість годин** - __120__ | _____обов'язкова_____<br>(обов'язкова, вибіркова) | |
| **Семестр викладання дисципліни** | ___6____<br>(порядковий номер семестру) | _____<br>(порядковий номер семестру) |
| **Вид контролю:** | _____екзамен_____<br>(залік, екзамен) | |
| **Розподіл часу:** | | |
| - лекції (годин) | 16 | ____ |
| - лабораторні роботи (годин) | _____ | ____ |
| - практичні заняття (годин) | 32 | ____ |
| - самостійна робота студентів (годин) | 42 | ____ |
| - курсовий проект (годин) | _____ | ____ |
| - курсова робота (годин) | _____ | ____ |
| - розрахунково-графічна робота (контрольна робота) | _____ | ____ |
| - підготовка та складання екзамену (годин) | __30___ | ____ |

**4. Очікувані результати навчання з дисципліни**

Основними завданнями вивчення дисципліни Безпека програм і даних є формування сукупності знань та вмінь для аналізу основних загроз безпеці програм та даних, типів атак, вивчення та використання основних методів кодування та шифрування даних, знання та використання різних криптографічних методів та систем захисту даних.

По завершені вивчення дисципліни студенти повинні володіти наступними компетентностями:

- здатність до пошуку, оброблення та аналізу інформації з різних джерел;
- здатність застосовувати знання у практичних ситуаціях;
- здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення;

[2] Якщо дисципліна викладається декілька семестрів, то на кожний семестр за відповідною формою навчання заповнюється окремий стовпчик таблиці.

[3] Якщо дисципліна на заочній (дистанційній) формі навчання не викладається, то графа "заочна форма навчання" відсутня.

- здатність до алгоритмічного та логічного мислення;
- здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

Результати навчання:

- аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки;
- уміння вибирати та використовувати відповідну задачі методологію створення програмного забезпечення;
- знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних;
- знати і застосовувати методи розробки алгоритмів, конструювання програмного забезпечення та структур даних і знань;
- знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

**5. Критерії оцінювання результатів навчання** Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі екзамену.

Відповідність підсумкової семестрової рейтингової оцінки в балах оцінці за національною шкалою та шкалою ECTS:

| Оцінка в балах | Оцінка за національною шкалою | Оцінка за шкалою ECTS | |
|---|---|---|---|
| | | Оцінка | Пояснення |
| 90-100 | Відмінно | A | Відмінно (відмінне виконання лише з незначною кількістю помилок) |
| 82 – 89 | Добре | B | Дуже добре (вище середнього рівня з кількома помилками) |
| 75 – 81 | | C | Добре (в загальному вірне виконання з певною кількістю суттєвих помилок) |
| 67 – 74 | Задовільно | D | Задовільно (непогано, але зі значною кількістю недоліків) |
| 60 – 66 | | E | Достатньо (виконання задовольняє мінімальним критеріям) |
| 35 – 59 | Незадовільно | FX | Незадовільно (з можливістю повторного складання) |
| 1 – 34 | | F | Незадовільно (з обов’язковим повторним курсом) |

**6. Засоби діагностики результатів навчання** тестові завдання.

**7. Розподіл дисципліни у годинах за формами організації освітнього процесу та видами навчальних занять[4]**

| Назва теми лекційного матеріалу | Кількість годин | | Назва тем | Кількість годин | | Література |
|---|---|---|---|---|---|---|
| | очна | заочна | ЛР, ПР, СЗ, СРС СРС | очна | заочна | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **Семестр 1.** | | | | | | |
| Тема 1. Вступ. Основи теорії захисту захисту інформації. | 2 | | ПР1. Вступ у кодування та шифрування. Криптоаналіз | 4 | | О. 1-8<br>Д. 1-5 |

[4] Якщо дисципліна викладається декілька семестрів, то теми розбивати посеместрово.

| | | | | | | |
|---|---|---|---|---|---|---|
| Класифікація загроз | | | простих шифрів.<br><br>СРС. Інформація, міри інформації, коди. | 5 | | |
| Тема 2. Кодування даних для комп'ютерних систем загального призначення | 2 | | ПР2. Методи кодування даних<br><br>СРС. Методи Лемпела-Зіва | 4<br><br>5 | | О. 1-8<br>Д. 1-5 |
| Тема 3. Методи криптографічного захисту даних. Шифри та їх використання. | 2 | | ПР3. Класичні методи та шифри<br><br>СРС. Класичні та сучасні методи а алгоритми шифрування даних | 4<br><br>6 | | О. 1-8<br>Д. 1-5 |
| Тема 4. Методи шифрування даних у комп'ютерних системах загального призначення, симетричні та асиметричні схеми шифрування. | 2 | | ПР4. Алгоритми та методи шифрування в комп'ютерних системах<br><br>СРС. Асиметричні методи шифрування та їх підтримка у бібліотеках мов програмування | 4<br><br>5 | | О. 1-8<br>Д. 1-5 |
| Тема 5. Безпека програм та даних на основі механізмів та політик розмежування прав доступу до даних | 2 | | ПР5. Використання хеш-функцій (на прикладі MD5), оцінка стійкості паролю до зламу<br><br>СРС. Використання хеш-функцій для захисту програм та даних | 4<br><br>5 | | О. 1-14<br>Д. 1-12 |
| Тема 6. Методи захисту даних та програм на основі алгоритмів приховування інформації в потоках даних | 2 | | ПР6. Методи приховування інформації в потоках даних<br><br>СРС. Стеганографія | 4<br><br>5 | | О. 1-14<br>Д. 1-12 |
| Тема 7. Методи захисту програм та даних під час виконання, захист носіїв даних. | 2 | | ПР7. Методи захисту виконуваних файлів (програм) від зламу та налагодження<br><br>СРС. Апаратні та програмні засоби захисту програм та даних | 4<br><br>5 | | О. 1-14<br>Д. 1-9 |
| Тема 8.Сучасні методи автентифікації та ідентифікації користувачів для захисту даних – цифровий підпис, біометричні методи автентифікації. | 2 | | ПР8. Електронний цифровий підпис на прикладі GnuPG, захист документів та електронної пошти за допомогою цифрових підписів<br><br>СРС. Інструментальні засоби захисту програм та даних | 4<br><br>5 | | О. 1-14<br>Д. 1-12 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | СРС<br>Підготовка до екзамену | 30 | | |
| **Усього за семестр** | 16 | | | 104 | | |
| **УСЬОГО за дисципліну** | 16 | | | 104 | | |

**8. Орієнтовна тематика індивідуальних та/або групових занять**

**9. Форми поточного та підсумкового контролю** усне та письмове опитування, захист практичних робіт, тестові завдання в системі Moodle.

**10. Інструменти, обладнання та програмне забезпечення** Debian GNU Linux, ОС Windows, GnuPG, C++, C#, Java, Python 3, GNU Octave/Scilab/Scicos/NSP.

**11. Рекомендовані джерела інформації**

**1. Базова література**


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.
12. Мнушка, О.В. Безпека програм і даних : конспект лекцій для студентів за спеціальністю 121 «Інженерія програмного забезпечення» / Мнушка О.В. - Харків, ХНАДУ, 2020.
13. Мнушка О.В. Методичні вказівки для проведення практичних робіт з дисципліни «Безпека програм і даних» для студентів за спеціальністю 121 «Інженерія програмного забезпечення» - Харків, ХНАДУ, 2020.
14. Мнушка О.В. Методичні вказівки для самостійної роботи з дисципліни «Безпека програм і даних» для студентів за спеціальністю 121 «Інженерія програмного забезпечення» - Харків, ХНАДУ, 2020.


**2. Допоміжна література**


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.
10. O. Mnushka and V. Savchenko, "Security Model of IOT-based Systems," 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2020, pp. 398-401, doi: 10.1109/TCSET49122.2020.235462.
11. Mnushka O.V., Savchenko V.M. Architecture models and patterns for safety and security for IOT applications // Комп’ютерні технології і мехатроніка. Збірник наукових праць за матеріалами міжнародної науково-практичної конференції. – Харків, ХНАДУ, 2019. – С. 30-33. – Режим доступу: https://dspace.khadi.kharkov.ua/dspace/bitstream/123456789/3032/1/Mnushka%20Savchenko%20%d0%9a%d0%a2%d0%9c_2019.pdf
12. Мнушка О.В., Савченко В.М. Модель безпеки інформаційної системи на базі технологій IoT / Мнушка О.В., Савченко В.М. // Вісник НТУ «ХПІ». Серія: Інформатика і моделювання. – Харків: НТУ «ХПІ». – 2019. – № 28 (1353). – С. 78 – 86. DOI: 10.20998/2411-0558.2019.28.09 – Режим доступу: https://dspace.khadi.kharkov.ua/dspace/handle/123456789/3030

## 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.

**Розроблено та внесено:** кафедрою комп'ютерних технологій та мехатроніки
(повне найменування кафедри)

**Розробник (и) програми:** старший викладач (підпис) Мнушка Оксана Василівна
(ПІБ розробників)

Обговорено та рекомендовано до затвердження на засіданні кафедри Протокол № 20 від "28" серпня 2020 р.
(номер) (та дата протоколу)

**Завідувач кафедри** д.т.н., проф. (підпис) Ніконов Олег Якович
(науковий ступінь, вчене звання) (ПІБ завідувача кафедри)

**Погоджено**

Декан Механічного факультету
(повна назва факультету, де читається дисципліна)

д.т.н., проф. (підпис) Кириченко Ігор Георгійович
(наук. ступінь, вчене звання) (ПІБ декана)

"31" 08 2020 року
(день) (місяць) (рік)



*Примітки:*

*Робоча програма навчальної дисципліни розробляється відповідною кафедрою у 2-х екземплярах на 5 років і затверджується до 30 серпня: 1 екземпляр – у навчальний відділ; 2-екземпляр залишається на кафедрі.*

***Форма в редакції ХНАДУ відповідно до листа МОН України за №1/9-434 від 09 липня 2018 року затверджена Методичною радою ХНАДУ 26 вересня 2018 року протокол №1***