ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ АВТОМОБІЛЬНО-ДОРОЖНІЙ УНІВЕРСИТЕТ
Система забезпечення якості освітньої діяльності та вищої освіти
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., проф.

_____ Ніконов О.Я.

СИЛАБУС
БЕЗПЕКА ПРОГРАМ І ДАНИХ / PROGRAM AND DATA SECURITY
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 2020

Автор: Алексієв О.П. професор кафедри комп’ютерних технологій і мехатроніки

Силабус розглянуто та затверджено на засіданні кафедри комп’ютерних технологій і мехатроніки, протокол № 20 від «28» серпня 2020 р.

СИЛАБУС

БЕЗПЕКА ПРОГРАМ І ДАНИХ /

PROGRAM AND DATA SECURITY

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: Алексієв Олег Павлович

- Професор викладач кафедри комп'ютерних технологій та мехатроніки;
- педагогічний стаж – 47 років
- контактний телефон +38-057-707-37-43
- e-mail: o.p.alex@gmail.com
- наукові інтереси: теоретичні та практичні питання програмної та комп'ютерної інженерії, комп'ютерні мережі, інформаційні техноло-гії керування, безпека даних

1.2. Асистент лектора:-

2. **Дисципліна** «Безпека програм і даних»

– рік навчання: 3;

– семестр навчання: 7;

– кількість годин за семестр: 150, в т. ч.

лекційних: 16;

практичних занять: 32;

на самостійне опрацювання: 102;

- 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 «Безпека програм і даних» 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: 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;
– 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, 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.

– знати і застосовувати методи розробки алгоритмів, конструювання програмного забезпечення та структур даних і знань.

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)**
Тема 1. Вступ. Основи теорії кодування даних. Кодування мультимедійних даних			
Загальні та спеціальні компетентності: – здатність застосовувати фундамен-	**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	2	

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
тальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення. – здатність до пошуку, оброблення та аналізу інформації з різних джерел *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.	5. Коригуючі коди. **Список рекомендованих джерел** Основний 1-8 Додатковий 1-5		
	Завдання для самостійної роботи: самостійне опрацювання літературних джерел, які зазначені у списку. *Питання, винесені на самостійне опрацювання:* інформація, міри інформації; коди.	10	4
	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
Тема 2. Поширені методи ефективного кодування даних для комп'ютерних систем загального призначення			
Загальні та спеціальні компетентності: – здатність до пошуку, оброблення та аналізу інформації з різних джерел – здатність застосовувати знання у	**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

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
практичних ситуаціях. – здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення. *Результати навчання* – 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. – здатність до алгоритмічного та логічного мислення.	**Завдання для самостійної роботи:** самостійне опрацювання літературних джерел, які зазначені у списку. *Питання, винесені на самостійне опрацювання:* методи стиснення даних; алгоритм Лемпеля-Зіва-Велча.	10	3
	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
Тема 3. Методи криптографічного захисту даних. Шифри та їх використання.			
Загальні та спеціальні компетентності: – здатність до пошуку, оброблення та аналізу інформації з різних джерел – здатність застосовувати знання у	**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

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
практичних ситуаціях. – здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення. *Результати навчання* – 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. здатність до алгоритмічного та логічного мислення.	**Завдання для самостійної роботи:** самостійне опрацювання літературних джерел, які зазначені у списку. *Питання, винесені на самостійне опрацювання:* класичні методи а алгоритми шифрування даних; сучасні методи а алгоритми шифрування даних.	11	3
	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
Тема 4. Методи шифрування даних у комп'ютерних системах загального призначення, симетричні та асиметричні схеми шифрування.			
Загальні та спеціальні компетентності: – здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в	**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

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
тому числі кібербезпеки). – 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. *Результати навчання* – 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. – 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,	**Завдання для самостійної роботи:** самостійне опрацювання літературних джерел, які зазначені у списку. *Питання, винесені на самостійне опрацювання:* стандарти шифрування даних; крипостійкість алгоритмів.	10	4
	Практична робота 4. Дослідження крипостійкості 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

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
конструювання програмного забезпечення та структур даних і знань.			
Тема 5 . Безпека програм та даних на основі механізмів та політик розмежування прав доступу до даних.			
Загальні та спеціальні компетентності: – здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки). – 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. *Результати навчання* – знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та	**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
	Завдання для самостійної роботи: самостійне опрацювання літературних джерел, які зазначені у списку. *Питання, винесені на самостійне опрацювання:* політики безпеки на локальному комп'ютері; політики безпеки у домені підприємства (організації)	10	4
	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

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
створюваних програмних систем. – 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.			
Тема 6. Методи захисту даних та програм на основі алгоритмів приховування інформації в потоках даних			
Загальні та спеціальні компетентності: – здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки). – 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	**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
	Завдання для самостійної роботи: самостійне опрацювання літературних джерел, які зазначені у списку. *Питання, винесені на самостійне опрацювання:* стеганографія; утиліти для кодування/декодування.	10	4
	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)
інженерії програмного забезпечення. *Результати навчання* – 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. – 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.	– виконання завдань; – презентація результатів роботи		
Тема 7. Методи захисту програм та даних під час виконання, захист носіїв даних.			
Загальні та спеціальні компетентності: – здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в	**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

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
тому числі кібербезпеки). – 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. *Результати навчання* – 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. – 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,	**Завдання для самостійної роботи:** самостійне опрацювання літературних джерел, які зазначені у списку. *Питання, винесені на самостійне опрацювання:* Апаратні та програмні засоби захисту програм та даних	5	2
	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

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
конструювання програмного забезпечення та структур даних і знань.			
Тема 8. Сучасні методи автентифікації та ідентифікації користувачів для захисту даних – цифровий підпис, біометричні методи автентифікації			
Загальні та спеціальні компетентності: – здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки). – 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. *Результати навчання* – знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та	**Лекція 3.** План лекції. 1. Цифровий підпис 2. Біометрична ідентифікація 3. Автентифікація на основі цифрових технологій 4. Автентифікація на основі біометричних даних. **Список рекомендованих джерел** Основний 1-11 Додатковий 1-9	2	1
	Завдання для самостійної роботи: самостійне опрацювання літературних джерел, які зазначені у списку. *Питання, винесені на самостійне опрацювання:* біометричні методи ідентифікації; біометричні методи автентифікації; проблеми використання біометричних методів ідентифікації та автентифікації;	6	4
	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

Результати навчання	**Навчальна діяльність**	**Робочий час студента (год.)**	**Оцінювання (бал)**
створюваних програмних систем. – 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.			
.	Підготовка до складання іспиту	30	1
Разом		**150** *годин/* **5** *кредитів*	**100** *балів*
Підсумковий контроль		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.

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.

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.

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

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: включає весь спектр письмових, усних, практичних контрольних процедур у залежності від компетентністних характеристик (знання, уміння, комунікація, автономність і відповідальність) результатів навчання, досягнення яких контролюється. Вимірювання рівня досягнення результатів навчання здійснюється коефіцієнтом засвоєння або експертно за критеріями, що корелюються з дескрипторами НРК. Вибір, конкретизація та деталізація критеріїв оцінювання з урахуванням специфіки освітніх

програм та їх компонентів здійснюється кафедрами на основі загальних критеріїв, наведених у СТВНЗ 7.1-01:2015 Положення про організацію освітнього процесу в ХНАДУ.

Під час вивчення дисципліни «Безпека програм і 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. Відпрацювання 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: повинні відповідати Морально-етичному кодексу учасників освітнього процесу Харківського національного автомобільно-дорожнього університету (З додатком згідно наказу ХНАДУ від 08 листопада 2019 № 147). Обов'язковим є:

– прагнути отримувати глибокі знання у відповідній області: сумлінно вчитися, не пропускати заняття без поважної причини, брати участь у навчальній та науково-дослідній роботах;

– прагнути максимально використовувати надані можливості з придбання теоретичних знань і практичних навичок з обраної спеціальності;

– виконувати вимоги, передбачені розпорядком дня університету, навчальними програмами, у суворо встановлені терміни;

– не користуватися забороненими допоміжними матеріалами і технічними засобами при проходженні процедур контролю знань, умінь і навичок, спиратися виключно на отримані знання;

не вчиняти дій, що перешкоджають здійсненню навчального процесу.

8.4. За порушення академічної доброчесності здобувачі вищої освіти можуть бути притягнені до академічної відповідальності у відповідності до Правил академічної доброчесності учасників освітнього процесу Харківського національного автомобільно-дорожнього університету (СТВНЗ 67.0-01:2019):

– повторне проходження оцінювання (контрольна робота, іспит, залік тощо);

– повторне проходження відповідного освітнього компонента освітньої програми;

– відрахування з університету;

– позбавлення академічної стипендії;

– позбавлення наданих університетом пільг з оплати навчання.