Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра геоінформаційних технологій
та космічного моніторингу Землі (№ 407)

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ С.І. Горелик
(підпис) (ініціали та прізвище)

«_27_» _____08_____ 2021 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист просторово-розподілених даних в комп'ютерних системах

(назва навчальної дисципліни)

Галузь знань: 10 Природничі науки
(шифр і найменування галузі знань)

Спеціальність: 103 Науки про Землю
(код та найменування спеціальності)

Освітня програма: Космічний моніторинг Землі
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Силабус введено в дію з 01.09.2021 року

Харків – 2021 р.

Розробник: Пащенко Р. Е., проф., д.т.н., проф. _____
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри геоінформаційних технологій та космічного моніторингу Землі. (№ 407)

Протокол № 1 від « 27 » серпня 2021 р.

Завідувач кафедри к.т.н., доц. _____ Горелик С.І.
(підпис)

Погоджено з представником здобувачів освіти:

Студентка гр 435ст Фоміних А.В.

1. Загальна інформація про викладача

Пащенко Руслан Едуардович, д.т.н., професор. З 2011 року викладає в університеті наступні дисципліни:

- захист просторово-розподілених даних в комп'ютерних системах;
- проектування баз геоданих;
- методи та методологія досліджень Землі та її геосфер;
- методи нелінійної динаміки в ГІС.

Напрями наукових досліджень: дослідження геофізичних сигналів і даних дистанційного зондування Землі з використанням методів нелінійної динаміки.

2. Опис навчальної дисципліни

Семестр, в якому викладається дисципліна – 5 семестр.

Обсяг дисципліни:

4,0 кредити ЄКТС (120 годин), у тому числі аудиторних – 56 годин, самостійної роботи здобувачів **–** 64 годин.

Форми здобуття освіти

Денна, дистанційна.

Дисципліна – обов’язкова.

Види навчальної діяльності – лекції, лабораторні роботи, самостійна робота здобувача.

Види контролю – поточний, модульний та підсумковий (семестровий) контроль (іспит).

Мова викладання – українська.

Необхідні обов’язкові попередні дисципліни (пререквізити) – вища математика, мікропроцесори та ЕОМ, інформатика та програмування.

Необхідні обов’язкові супутні дисципліни (кореквізити) – основи роботи в Інтернет та інформаційні мережі, математичні методи і моделі.

3. Мета та завдання навчальної дисципліни

Мета

Вивчення навчальної дисципліни «Захист просторово-розподілених даних в комп'ютерних системах» полягає у придбанні студентами базових знань про джерела витоку інформації та сучасні методи захисту просторово-розподілених даних в комп'ютерних системах, а також набуття практичних навичок з створення систем захисту просторово-розподілених даних в комп'ютерних системах.

Завдання

Вивчення дисципліни є опанування методів захисту просторово-розподілених даних в комп'ютерних системах.

Після опанування дисципліни здобувач набуде наступні **компетентності**:

ЗК1 – здатність застосовувати знання в практичних ситуаціях.
ЗК5 – здатність використання інформаційних технологій.
ЗК6 – здатність вчитися і бути сучасно освіченим, усвідомлювати можливість навчання впродовж життя.
ЗК7 – здатність працювати як самостійно, так і в команді.
ЗК8 – навички забезпечення безпеки життєдіяльності.
ЗК10 – визнання морально-етичних аспектів досліджень і необхідності інтелектуальної чесності, а також професійних кодексів поведінки.
ФК2 – здатність застосовувати базові знання фізики, хімії, біології, екології, математики, інформаційних технологій тощо при вивченні Землі та її геосфер.
ФК3 – здатність використовувати знання з загальних інженерних наук у навчанні та професійній діяльності, вміння використовувати їх теорії, принципи та технічні підходи.
ПРН5 – використовувати методи збирання інформації в галузі геодезії і землеустрою, її систематизації і класифікації відповідно до поставленого проектного або виробничого завдання.
ПРН9 – обробляти результати геодезичних вимірювань, топографічних і кадастрових знімань, з використанням геоінформаційних технологій та комп’ютерних програмних засобів і системи керування базами даних.

Очікується, що після опанування дисципліни здобувач будуть досягнуті наступні **результати навчання** і він буде знати:

- потенційні загрози та канали витоку інформації;
- типи шкідливих програм;
- основи безпеки в мережі Internet;
- основи побудови систем захисту інформації;
- математичні моделі систем та процесів захисту інформації;
- програмно-технічні методи захисту інформації;
- технологію брандмауерів.

4. Зміст навчальної дисципліни

Модуль 1.

Змістовний модуль 1. Захист від шкідливих програм і безпека в мережі Internet

Тема 1. Вступ до дисципліни «Захист просторово-розподілених даних в комп'ютерних системах»

- *Форма занять: лекція, самостійна робота.*
- *Обсяг аудиторного навантаження: 2 години.*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): відсутні.*

Загальні відомості про дисципліну. Методична побудова навчальної дисципліни «Захист просторово-розподілених даних в комп'ютерних системах» і зв'язок з іншими дисциплінами. Значення курсу у фаховій підготовці. Інформаційно-методичне забезпечення дисципліни. Актуальність проблеми захисту інформації.

Обсяг самостійної роботи здобувачів: 1 година.

Опрацювання матеріалу лекцій. Формування питань до викладача. Актуальність проблеми захисту інформації.

Тема 2. Законодавчі та правові аспекти захисту просторово-розподілених даних в комп'ютерних системах

- *Форма занять: лекція, самостійна робота.*
- *Обсяг аудиторного навантаження: 2 години*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): відсутні.*

Нормативно-правова база для організації та проведення дій щодо захисту просторово-розподілених даних в комп'ютерних системах. Задачі, які вирішуються в Україні при побудові системи безпеки інформації. Закони, що регламентують використання, розповсюдження та зберігання інформації в Україні. Закордонне нормативно-правове забезпечення захисту інформації.

- *Обсяг самостійної роботи здобувачів: 1 година.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Вимоги закону України «Про інформацію».

Тема 3. Шкідливі програми

- *Форма занять: лекція, лабораторна робота, самостійна робота.*
- *Обсяг аудиторного навантаження: 16 годин.*
- *Лабораторна робота: «Дослідження методів парольного захисту інформації».*
- *Лабораторна робота: «Аналіз правил вибору паролів та зниження їх уразливості».*

- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): персональні комп'ютери, спеціальне програмне забезпечення.*

Класифікація шкідливих програм Історія створення і розповсюдження шкідливих програм. Тенденції розвитку шкідливих програм. Сучасна класифікація вірусних програм. Методи зараження COM-файлів і EXE-файлів та боротьба з ними. Основні риси троянських програм та програмних закладок. Методи виявлення шкідливих програм.

- *Обсяг самостійної роботи здобувачів: 14 годин.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Тенденції розвитку шкідливих програм. Вплив шкідливих програм на роботу комп'ютерних системах. Програми виявлення шкідливих програм.

Тема 4. Безпека в мережі Internet

- *Форма занять: лекція, лабораторна робота, самостійна робота.*
- *Обсяг аудиторного навантаження: 13 годин.*
- *Лабораторна робота: «Дослідження методів захисту інформації за допомогою брандмауера».*
- *Лабораторна робота: «Аналіз та порівняння схем побудови брандмауерів».*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): персональні комп'ютери, спеціальне програмне забезпечення.*

Класифікація можливих каналів витікання інформації в мережі Internet. Типові сервіси, структура портів, загрози для протоколів та служб Internet, аутентифікація, маскування під інших користувачів, потенційні проблеми з електронною поштою. Методи і засоби забезпечення безпеки у мережі Internet.

- *Обсяг самостійної роботи здобувачів: 12 годин.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Можливі канали витікання інформації в мережі Internet. Протоколи та служби мережі Internet. Засоби забезпечення безпеки у мережі Internet.

Модульний контроль 1

- *Форма занять: написання модульної роботи в аудиторії (за рішенням лектора допускається проведення у дистанційній формі).*
- *Обсяг аудиторного навантаження: 1 година*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): відсутні.*
- *Обсяг самостійної роботи здобувачів – за необхідністю.*

Підготовка до модульного контролю.

Змістовний модуль 2. Криптографічні методи та засоби захисту інформації

Тема 5. Програмні методи захисту інформації

- *Форма занять: лекція, лабораторна робота, самостійна робота.*
- *Обсяг аудиторного навантаження: 8 годин.*
- *Лабораторна робота: «Дослідження ранніх методів криптографічного захисту текстової інформації».*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): відсутні.*

Моделі інформаційної взаємодії. Криптографічні методи та засоби захисту інформації, захист даних при передаванні по каналах зв'язку, захищений обмін даними, захист електронної пошти. Ранні етапи розвитку криптографії. Класифікація криптографічних методів.

- *Обсяг самостійної роботи здобувачів: 12 годин.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Етапи розвитку криптографії. Криптографічні методи та засоби захисту.

Тема 6. Технології криптозахисту

- *Форма занять: лекція, лабораторна робота, самостійна робота.*
- *Обсяг аудиторного навантаження: 11 годин.*
- *Лабораторна робота: «Дослідження методів комп'ютерного криптографічного захисту інформації».*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): відсутні.*

Технології симетричного криптозахисту. Криптосистема з симетричним ключем. Блочні шифри DES та AES. Поняття абсолютно стійкого шифру. Вимоги до системи з абсолютною стійкістю. Технології асиметричного криптозахисту. Криптосистема з асиметричним ключем. Алгоритм «рюкзака». Хеш-функції. Шифр RSA.

- *Обсяг самостійної роботи здобувачів: 16 годин.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Технології симетричного криптозахисту. Технології асиметричного криптозахисту.

Тема 7. Технології електронного підпису

- *Форма занять: лекція, самостійна робота.*
- *Обсяг аудиторного навантаження: 2 години.*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): відсутні.*

Аутентифікація сповіщення при захисті передачі та зберіганні даних від розповсюдження та зміни. Класифікація схем цифрового підпису. Схеми

цифрового підпису з відновленням сповіщення. Схеми цифрового підпису з додаванням. Інфраструктура відкритого ключа.

- *Обсяг самостійної роботи здобувачів: 8 годин.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Схеми цифрового підпису з відновленням сповіщення. Схеми цифрового підпису з додаванням.

Модульний контроль 2

- *Форма занять: написання модульної роботи в аудиторії (за рішенням лектора допускається проведення у дистанційній формі).*
- *Обсяг аудиторного навантаження: 1 година*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): відсутні.*
- *Обсяг самостійної роботи здобувачів – за необхідністю.*

Підготовка до модульного контролю.

5. Індивідуальні завдання

6. Методи навчання

Використовуються наступні методи навчання: словесні (пояснення, розповідь, бесіда тощо), наочна (демонстрування) та практичні (лабораторні роботи).

7. Методи контролю

Поточний контроль (теоретичне опитування й розв'язання практичних завдань), модульний контроль (тестування за розділами курсу) та підсумковий (семестровий) контроль (іспит). Форма проведення іспиту – письмово-усна.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Активність під час аудиторної роботи	0…1	7	0…5 (максимальна кількість балів за цим показником)
Виконання і захист лабораторних робіт	0…8	4	0…32
Модульний контроль	0…20	1	0…20
Змістовний модуль 2			
Активність під час аудиторної роботи	0…1	5	0…5 (максимальна кількість балів за цим показником)

Виконання і захист лабораторних робіт	0…9	2	0…18
Модульний контроль	0…20	1	0…20
За семестр			**0…100**

Прийнята шкала оцінювання

Сума балів за всі види навчальної діяльності	Оцінка для екзамену, *курсового проекту* (роботи), практики
90-100	відмінно
75-89	добре
60-74	задовільно
01-59	незадовільно з можливістю повторного складання

Білет для іспиту складається з двох теоретичних та одного практичного запитання. Теоретичне запитання оцінюються по 30 б кожен, практичне – 40 б. Загалом 100 б. Під час складання семестрового іспиту здобувач має можливість отримати максимум 100 балів.

Критерії оцінювання роботи здобувача протягом семестру

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх.

«відмінно» – відповідає високому (творчому) рівню компетентності:

- Студент виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили;

Добре (75-89). Твердо знати мінімум, захистити всі індивідуальні завдання, виконати всі КР , здати тестування та поза аудиторну самостійну роботу.

«добре» – отримує Студент за двома рівнями оцінювання залежно від набраної кількості балів та відповідає достатньому (конструктивно-варіативному) рівню компетентності:

- Студент вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв’язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна;

- Студент вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок;

Задовільно (60-74). Показати мінімум знань та умінь. Захистити всі індивідуальні завдання та здати тестування.

«задовільно» – отримує Студент за двома рівнями оцінювання залежно від набраної кількості балів та відповідає середньому (репродуктивному) рівню компетентності:

- Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих;

- Студент володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні

Незадовільно (0-59) – відповідає низькому (рецептивно-продуктивному) рівню компетентності:

- Студент не опанував навчальний матеріал дисципліни, не знає наукових фактів, визначень, майже не орієнтується в першоджерелах та рекомендованій літературі, відсутні наукове мислення, практичні навички не сформовані.

9. Політика навчального курсу

Відпрацювання пропущених занять відбувається відповідно до розкладу консультацій, за попереднім погодженням з викладачем. Питання, що стосуються академічної доброчесності, розглядає викладач або за процедурою, визначеною у Положенні про академічну доброчесність.

10. Методичне забезпечення та інформаційні ресурси

Підручники, навчальні посібники, навчально-методичні посібники, конспекти лекцій, методичні рекомендації з проведення лабораторних робіт тощо, які видані в Університеті знаходяться за посиланням:

http://library.khai.edu/library/fulltexts/doc/_AA_Zahist_Prostorovo.pdf

Сторінка дисципліни знаходиться за посиланням:

https://mentor.khai.edu/course/view.php?id=3335

11. Рекомендована література

Базова

1. Пащенко Р.Е. Захист просторово-розподілених даних в комп’ютерних системах. Конспект лекцій / Пащенко Р.Е. – Х.: НАКУ ім. М.Є. Жуковського “ХАІ”, 2020. – 104 с.

2. Кузнецов О. О. Захист інформації в інформаційних системах / Кузнецов О. О., Євсеєв С. П., Король О. Г. – Х. : Вид. ХНЕУ, 2011. – 512 с.

3. Завгородний В. И. Комплексная защита информации в компьютерных системах / В. И. Завгородний. – М. : Логос, ПБОЮЛ Н.А. Егоров, 2001. – 264 с.
4. Остапов С. Е. Технології захисту інформації : навчальний посібник / Остапов С. Е., Євсеєв С. П., Король О. Г. – Х. : Вид. ХНЕУ, 2013. – 476 с.
5. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії : навч. посібн. / Кузнецов О. О., Євсеєв С. П., Король О. Г. – Х. : Вид. ХНЕУ, 2010. – 316 с.

Допоміжна

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Видавнича група BHV, 2009. – 608 с.
2. Кавун С. В. Основи інформаційної безпеки / Кавун С. В., Смірнов О. А., Столбов В. Ф. – Кіровоград : Вид. КНТУ, 2012. – 414 с.
3. Ємець В. Сучасна криптографія. Основні поняття / Ємець В., Мельник А., Попович Р. – Львів : Бак, 2003. – 144 с.
4. Баричев С. Г. Основы современной криптографии / С. Г. Баричев, Р. Е. Серов – М. : Горячая линия – Телеком, 2001. – 152 с.