Український державний університет залізничного транспорту

Рекомендовано
на засіданні кафедри
Спеціалізованих комп'ютерних систем
прот. № 1 від 18.09.2023 р.

Завідувач кафедри СКС

_____Мойсеєнко В.І.

СИЛАБУС З ДИСЦИПЛІНИ

Криптографічний захист інформації

I-II семестри 2023-2024 навчального року

освітній рівень перший (бакалавр)

галузь знань 17 – Електроніка, автоматизація та

електронні комунікації

Спеціальність 174 Автоматизація, комп'ютерно –

інтегровані технології та робототехніка

Освітні програми: Комп'ютерно – інтегровані технології та хмарні сервіси
Час та аудиторія проведення занять: Згідно розкладу - http://rasp.kart.edu.ua/

1. Команда викладачів:

Лектор:
Павленко Євген Петрович (кандидат технічних наук, доцент),
Контакти: *+38 (057) 730-10-61,* e-mail: *pavlenko@ kart.edu.ua*

Години прийому та консультації: кожен понеділок з 13.00-14.00
Розміщення кафедри: Місто Харків, майдан Фейєрбаха, 7, 3 корпус, 4 поверх, 431 аудиторія.
Веб сторінка курсу: http://kart.edu.ua/kafedra-sks-ua/pro-kafedru-sks-ua
Додаткові інформаційні матеріали: http://metod.kart.edu.ua

Харків – 2023

Сутність захисту інформації полягає у виявленні, усуненні або нейтралізації негативних джерел, причин і умов впливу на інформацію. Ці джерела становлять загрозу безпеці інформації. Цілі і методи захисту інформації відображають її сутність.

У цьому сенсі захист інформації ототожнюється з процесом забезпечення інформаційної безпеки, як глобальної проблеми безпечного розвитку світової цивілізації, держав, спільноти людей, окремої людини, існування природи.

Вивчаючи цей курс, студенти не тільки зрозуміють найбільш поширені загрози безпеки інформаційних систем та мереж, а також основні функції сервісних служб захисту даних та ресурсів, але й навчаться вибрати алгоритм шифрування даних як засіб їх захисту від несанкціонованого доступу; від залежності від умов передачі даних вибрати методи та протоколи аутентифікації і ключового обміну.

Курс має на меті сформувати та розвинути наступні компетентності студентів:

1. **Ціннісно-смислову компетентність** (формування та розширення світогляду студента в галузі захисту інформації, здатність до розуміння важливості використання алгоритмів шифрування та протоколів аутентифікації);
2. **Загальнокультурну компетентність** (розуміння культурних, історичних та регіональних особливостей, що склалися в Україні та за її межами в галузі захисту інформації та завадостійкого кодування);
3. **Навчально-пізнавальну компетентність** (формування у студента зацікавленості про стан та перспективи розвитку методів стискання та шифрування даних, проблеми їх використання з метою розвитку креативної складової компетентності; вміння знаходити рішення у нестандартних ситуаціях в контексті попередження та виявлення загроз інформаційній безпеці)
4. **Інформаційну компетентність** (розвиток вмінь студента до самостійного пошуку, аналізу, структурування та відбору потрібної інформації в галузі захисту інформації за допомогою сучасних інформаційних технологій)
5. **Комунікативну компетентність** (розвиток у студента навичок роботи в команді шляхом реалізації групових проектів в галузі захисту інформації, вміння презентувати власний проект та кваліфіковано вести дискусію у цій сфері).

Чому ви маєте обрати цей курс?

Якщо вас цікавлять комп’ютерні системи та мережі, системне програмування, спеціалізовані комп’ютерні системи, захист інформації, засоби завадостійкого кодування та стиску даних, вам потрібна саме ця дисципліна!

Від здобувачів очікується: базове розуміння математики, дискретної математики, прикладної теорії цифрових автоматів, інформатики, комп’ютерної електроніки та схемотехніки, а також обізнаність в питаннях комп’ютерних мережевих технологій та програмної інженерії, необхідних для проектування та розробки комп’ютерних систем, тобто апаратного та програмного забезпечення.

Перша частина курсу присвячена огляду безпеки комп’ютерних систем та шкідливого програмного забезпечення, засобам завадостійкого кодування, друга частина присвячена криптографії та протоколам аутентифікації.

Команда викладачів і ваші колеги будуть готові надати будь-яку допомогу з деякими з найбільш складних аспектів курсу по електронній пошті, на форумі і особисто - у робочий час.

Огляд курсу

Цей курс, який вивчається з вересня по травень, дає студентам глибоке розуміння методів та засобів кодування та захисту інформації - від традиційних до сучасних та можливостей подальшого застосування її потенціалу для потреб залізничного транспорту України.

Курс складається з однієї лекції на тиждень, одного практичного заняття раз у два тижні, одної лабораторної роботи раз у два тижні. Він супроводжується текстовим матеріалом, презентаціями та груповими завданнями. Студенти матимуть можливість застосовувати отримані знання та вирішувати практичні завдання протягом обговорень в аудиторії та розробки проекту із захисту інформації для залізниці. В рамках курсу передбачають лекції запрошених роботодавців з ІТ-компаній.

Теорія кодування та захист інформації в комп'ютерних системах / схема курсу

<table>
<tr><td rowspan="10">Поміркуй</td><td>Лекції</td><td></td></tr>
<tr><td>Запрошені лектори</td><td></td></tr>
<tr><td>Довідковий матеріал</td><td></td></tr>
<tr><td>Презентації</td><td></td></tr>
<tr><td>Обговорення в аудиторії</td><td rowspan="8">Виконай</td></tr>
<tr><td>Групові завдання</td></tr>
<tr><td>Екскурсії</td></tr>
<tr><td>Індивідуальні консультації</td></tr>
<tr><td>Онлайн форум (якщо він є)</td></tr>
<tr><td>Залік</td></tr>
</table>

Практичні заняття курсу передбачають виконання групових проектів із захисту інформації для потреб залізниці (групи від 2х до 3 осіб) та презентацію власних проектів в кінці курсу. Проект фіналізується короткою роботою. Виконання завдання супроводжується зануренням у суміжні дисципліни, що доповнюють теми, та формує у студента інформаційну та комунікативну компетентності.

Ресурси курсу

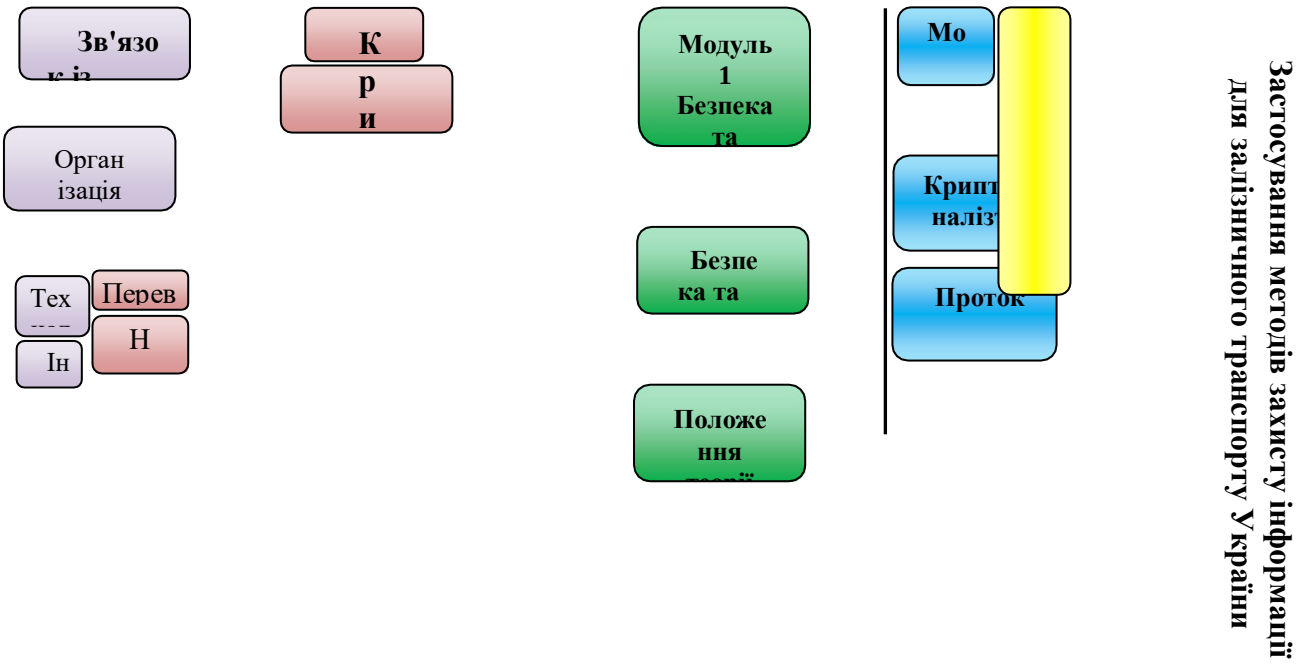
Інформація про курс, додатковий матеріал та посилання на електронні ресурси доступні на сайті Університету у розділі «дистанційне навчання», включаючи навчальний план, лекційні матеріали, презентації, завдання та правила оцінювання курсу поряд із питаннями, над якими необхідно поміркувати під час підготовки для обговорення в аудиторії. Необхідна підготовка повинна бути завершена до початку наступної лекції. Підчас обговорення ми запропонуємо вам критично поміркувати над тим, як використовуються методи та засоби захисту інформації в Україні та світі та як пристосувати альтернативні та сучасні методи та засоби захисту інформації до потреб залізничного транспорту. Студент повинен бути готовим до дискусій.

Приклади питань для обговорення доступні на слайдах відповідних презентацій.

Ось деякі з них:

1. Класифікація засобів захисту інформації. Історичні етапи розвитку. Цілі і завдання.
2. Санкціонований та несанкціонований доступ. Загрози безпеки інформаційних систем.
3. Шкідливе програмне забезпечення, його різновиди.
4. Типові атаки інформації в мережі.
5. Основні принципи організаційного захисту інформації.
6. Поняття завадостійкого кодування. Коректуючі коди.
7. Шифри однозначної заміни. Поліграмні шифри.
8. Які існують протоколи аутентифікації?

Теми курсу



№	Тематичні критерії (теми дисципліни)
Модуль №1 Безпека та захист даних. Теорія кодування.	
1.1	Безпека та захист даних.
1.2	Положення теорії кодування.
Модуль №2 Мережева безпека.	
2.1	Криптоаналіз та криптографія.
2.2	Протоколи аутентифікації.

Міждисциплінарні зв’язки

Дисципліна базується на основних положеннях курсів «Організація та системи керування БД», «Технології автоматизації проектування комп’ютерних систем та мереж», «Інженерія ПЗ». В свою чергу, її положення використовуються при викладанні предмету «Методологія контролю та діагностики комп’ютерних систем та мереж».

Лекції та практичні заняття

Список основних лекцій курсу наведений нижче. Пильнуйте за змінами у розкладі.

Тиждень	Кількість годин	Тема лекції	Кількість годин	Тема практичних, семінарських та лабораторних занять
1			2	ПР-1 Основи інформаційної безпеки. Традиційні алгоритми шифрування (початок)
2	2	Лекц.№1. Огляд безпеки системи	2	ЛР-1 Огляд безпеки системи (початок)
3			2	ПР-1 (закінчення)
4	2	Лекц.№2. Механізми і політики розмежування прав доступу	2	ЛР-1 (закінчення)
5			2	ПР-2 Афінна система підстановок Цезаря (початок)
6	2	Лекц.№3. Шкідливе програмне забезпечення	2	ЛР-2 Модель загроз інформаційної безпеки. Модель порушника інформаційної безпеки
7			2	ПР-2 (закінчення)
8	2	Лекц.№4. Завадостійке кодування. Параметри коректуючих кодів	2	ЛР-2 (закінчення)
		Модульний контроль знань		
9			2	ПР-3 Коди Хемінга (початок)
10	2	Лекц.№5. Коди Хемінга. Циклічні коди	2	ЛР-3 Шифри перестановки та заміни (початок)
11			2	ПР-3 (закінчення)
12	2	Лекц.№6 Захист, доступ та аутентифікація	2	ЛР-3 (закінчення)
13			2	ПР-4 Шифрування за допомогою методів Віженера та гамування (початок)
14	2	Лекц.№7 Моделі захисту. Захист пам’яті	2	ЛР-4 Шифри гамування
15			2	ПР-4 (закінчення)
		Модульний контроль знань		

ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Вивчивши цей курс, студент:

- сформує основні поняття та термінологію теорії кодування;
- матиме уявлення про методологію формування сучасних інформаційних технологій як цілеспрямовану інтеграцію процесів передачі та обробки даних на основі використання засобів ОТ і зв'язку;
- набуде знань про найбільш поширені загрози безпеки інформаційних систем та мереж, а також основні функції сервісних служб захисту даних та ресурсів,
- набуде здатності обґрунтовано вибрати алгоритм шифрування даних як засіб їх захисту від несанкціонованого доступу;
- набуде компетентності щодо застосування сучасного програмного забезпечення для захисту інформації;
- сформує власний світогляд в галузі захисту інформації, орієнтований на сучасні потреби суспільства;
- матиме уявлення про проблеми забезпечення інформаційної безпеки електронного бізнесу та електронної комерції;
- набуде здатності до самостійного пошуку, аналізу, структурування та відбору потрібної інформації в галузі захисту інформації, безпечності спеціалізованих комп'ютерних систем;
- набуде компетентності особистісного самовдосконалення, фізичного, духовного й інтелектуального саморозвитку, емоційної саморегуляції, підтримки постійної жаги до самовдосконалення та самопізнання проблем безпеки інформації спеціалізованих комп'ютерних систем.

Правила оцінювання

При заповненні заліково-екзаменаційної відомості та залікової книжки (індивідуального навчального плану) студента, оцінка, виставлена за 100-бальною шкалою, повинна бути переведена до національної шкали (5, 4, 3,) та шкали ECTS (A, B, C, D, E)

Визначення назви за державною шкалою(оцінка)	Визначення назви за шкалою ECTS	За 100 бальною шкалою	ECTS оцінка
ВІДМІННО – 5	**Відмінно** – відмінне виконання лише з незначною кількістю помилок	90-100	A
ДОБРЕ – 4	**Дуже добре** – вище середнього рівня з кількома помилками	82-89	B
	Добре – в загальному правильна робота з певною кількістю грубих помилок	75-81	C
ЗАДОВІЛЬНО - 3	**Задовільно** - непогано, але зі значною кількістю недоліків	69-74	D

	Достатньо – виконання задовольняє мінімальні критерії	60-68	E
НЕЗАДОВІЛЬНО - 2	**Незадовільно** – потрібно попрацювати перед тим як отримати залік (без повторного вивчення модуля)	35-59	FX
	Незадовільно - необхідна серйозна подальша робота (повторне вивчення модуля)	<35	F

Завдання на самостійну роботу:

- Студентам пропонується обрати один з варіантів тем для створення власного проекту впродовж семестру. За вчасне та вірне виконання завдання нараховується **20 балів до поточного модульного контролю**. За вчасне та частково вірне виконання – від 15 до 25 балів. За невиконане завдання бали не нараховуються. Необхідний обсяг виконання завдання складає 50% на перший модульний контроль і 100% на другий модульний контроль. Перебіг поточного виконання завдання та питання для обговорення надсилаються на e-mail викладача або перевіряються ним особисто.
- Студенти мають прорецензувати одну роботу іншого студента або групи впродовж семестру та висловити свої критичні зауваження.

	Теми проектів
1	Протоколи контролю цілісності.
2	Код з перевіркою на парність. Основні параметри коректуючих кодів.
3	Циклічні коди.
4	Шифри перестановки
5	Протоколи аутентифікації в комп'ютерних системах
6	Різновиди блочного комбінованого шифрування

Відвідування лекцій:

Бали за цю складову нараховуються взагалі, якщо студент не відвідував більш 50% лекційних занять у модулі без поважних причин. За відвідування кожної лекції нараховується 1 бал. **Максимальна сума становить 15 балів**.

Пропущені студентом лекції вивчаються самостійно згідно теми та наданої викладачем літератури.

Для відпрацювання пропущених лабораторних занять студент повинен звернутися до викладача й отримати відповідне завдання.

Консультації відбуваються відповідно до наданого графіку, або в он-лайн режимі через Інтернет-мережу.

Ступінь залученості:

Мета участі в курсі – залучити вас до дискусії, розширити можливості навчання для себе та своїх однокурсників та дати вам ще один спосіб перевірити свої погляди на питання застосування сучасних технологій **захисту інформації** для

залізничного транспорту. Участь буде оцінюватися на основі кількості та вірності ваших відповідей. Питання, хоча й заохочуються, однак не оцінюються в цьому блоці. Ми намагаємося надати всім студентам рівні та справедливі можливості для підвищення власною залученості. **Максимальна сума становить 10 балів**.

Практичні заняття:

Оцінюються за відвідуваннями (до 3 балів), ступенем залученості (до 7 балів) та стислою презентацією виконаного завдання (до 5 балів). Ступінь залученості визначається участю у роботі дискусійного клубу з питань **захисту інформації** для залізничного транспорту. **Максимальна сума становить 15 балів**.

Модульне тестування:

Оцінюються за вірними відповідями на тестові модульні питання (20 питань в тесті, кожна вірна відповідь оцінюється в 2 бали). **Максимальна кількість становить 40 балів за модуль**.

Залік: (Іспит)

- Студент отримує залік (іспит) за результатами модульного 1-го та 2-го контролю шляхом накопичення балів. Максимальна кількість балів, яку може отримати студент становить 100 (до 60 балів поточного контролю та до 40 балів тестування). Середнє арифметичне суми модульних оцінок складає заліковий бал. Якщо студент не погоджується із запропонованими балами він може підвищити їх на заліку, відповівши на питання викладача (дати посилання на перелік залікових питань або їх список)

Команда викладачів:

Павленко Євген Петрович (http://kart.edu.ua/kafedra-ckc-ua/kolectuv-kafedru-sks-ua/pavlenko-ep-ua) - викладач з дисципліни **Теорія кодування та захист інформації** в УкрДУЗТ. Отримав ступінь к.т.н. за спеціальністю 05.13.09 – Математичне та програмне забезпечення обчислювальних машин та систем у ХНУРЕ у 1995 році. Напрямки наукової діяльності: розробка та тестування програмного забезпечення інформаційних систем.

Кодекс академічної доброчесності

Порушення Кодексу академічної доброчесності Українського державного університету залізничного транспорту є серйозним порушенням, навіть якщо воно є ненавмисним. Кодекс доступний за посиланням:

http://kart.edu.ua/documentu-zvo-ua

Зокрема, дотримання Кодексу академічної доброчесності УкрДУЗТ означає, що вся робота на іспитах та заліках має виконуватися індивідуально. Під час виконання самостійної роботи студенти можуть консультуватися з викладачами та з іншими студентами, але повинні самостійно розв'язувати завдання, керуючись власними знаннями, уміннями та навичками. Посилання на всі ресурси та джерела (наприклад, у звітах, самостійних роботах чи презентаціях) повинні бути чітко визначені та оформлені належним чином. У разі спільної роботи з іншими студентами над виконанням індивідуальних завдань, ви повинні зазначити ступінь їх залученості до роботи.

Інтеграція студентів із обмеженими можливостями

Вища освіта є провідним чинником підвищення соціального статусу, досягнення духовної, матеріальної незалежності і соціалізації молоді з обмеженими функціональними можливостями й відображає стан розвитку демократичних процесів і гуманізації суспільства.

Для інтеграції студентів із обмеженими можливостями в освітній процес Українського державного університету залізничного транспорту створена система дистанційного навчання на основі сучасних педагогічних, інформаційних, телекомунікаційних технологій.

Доступ до матеріалів дистанційного навчання з цього курсу можна знайти за посиланням: http://do.kart.edu.ua/