Український державний університет залізничного транспорту

Рекомендовано
на засіданні кафедри
транспортного зв'язку
прот. № 1 від 27.08.2020 р.

СИЛАБУС З ДИСЦИПЛІНИ

МЕРЕЖЕВА БЕЗПЕКА

Освітній рівень перший (бакалаврський)

Галузь знань 17 Електроніка та телекомунікації

Спеціальність 172 Телекомунікації та радіотехніка

Освітня програма Телекомунікаційні системи та мережі

Проведення занять згідно розкладу http://rasp.kart.edu.ua/

Команда викладачів:

Лектор: Лисечко Володимир Петрович (кандидат технічних наук, доцент), Контакти: +38 (057) 730-10-81, e-mail: tz@kart.edu.ua
Асистент лектора: Лисечко Володимир Петрович (кандидат технічних наук, доцент), Контакти: +38 (057) 730-10-81, e-mail: tz@kart.edu.ua Години прийому та консультації: понеділок з 14.10-15.30
Веб сторінка курсу: http://do.kart.edu.ua/ Додаткові інформаційні матеріали: http://metod.kart.edu.ua

Харків

Огляд курсу

Цей курс, який вивчається протягом одного семестру, дає студентам глибоке розуміння інноваційних підходів та технологій у сфері захисту інформації в телекомунікаційних мережах залізничного транспорту. Метою курсу є навчання студентів основним методам, принципам, способам управління інформаційною безпекою, з урахуванням можливих впливів порушників та прогнозу розвитку методів порушення безпеки інформації. Цей курс формує базові знання з проблем теорії та практики захисту інформації, в ньому розглядаються основні протиріччя забезпечення безпеки інформації та методи їх вирішення.

Курс складається з лекцій та практичних занять. Курс супроводжується пояснювально-ілюстративним матеріалом. Студенти матимуть можливість застосовувати отримані знання та вирішувати практичні завдання протягом обговорень на заняттях.

Ресурси курсу

Інформація про курс розміщена на сайті Університету (http://metod.kart.edu.ua/), включаючи навчальний план, матеріали, завдання та правила оцінювання курсу).

Додатковий матеріал та посилання на електронні ресурси доступні на сайті Університету у розділі «дистанційне навчання» поряд із питаннями, над якими необхідно поміркувати підчас підготовки для обговорення на заняттях. Необхідна підготовка повинна бути завершена до початку наступного заняття. Підчас обговорення ми запропонуємо Вам критично поміркувати над тим, як використовуються інноваційні підходи та технології при побудові об’єктів інфокомунікаційної інфраструктури залізничного транспорту та їх комплексів з точки зору захисту інформації. Ви повинні бути готовими до дискусій та мозкових штурмів – ми хочемо знати, що Ви думаєте!

Теми курсу

Модуль 1

Змістовий модуль 1. Основні положення управління інформаційною безпекою.

Тема 1. Основні поняття та визначення інформаційної безпеки.

Вступ. Предмет, ціль і задачі курсу. Структура та зміст навчальної дисципліни. Порядок, засоби діагностики та успішності вивчення. Основні поняття та визначення інформаційної безпеки. Проблеми захисту інформації від несанкціонованого доступу.

Тема 2. Нормативно-правове забезпечення інформаційної безпеки.

Нормативно-правове забезпечення інформаційної безпеки. Нормативно-правові документи верхнього рівня. Нормативно-правові документи середнього рівня. Нормативно-правові документи нижнього рівня. Нормативні документи з технічного захисту інформації України. Загальні положення щодо захисту від НСД.

Змістовий модуль 2. Побудова систем захисту інформації

Тема 3. Визначення інформації, що підлягає захисту.

Класифікація інформації, що підлягає захисту. Визначення інформаційних та програмно-технічних ресурсів, що підлягають захисту. Відомості, що становлять комерційну таємницю. Захист державної таємниці.

Тема 4. Загрози і канали витоку інформації.

Загрози і канали витоку інформації. Загрози для об'єктів ІС. Загрози для процесів, процедур і програм обробки інформації. Загрози для інформації в каналах зв'язку. Загрози інформації, що виникають при побічних електромагнітних випромінюваннях і наводках.

Загрози для механізмів управління системою захисту. Проведення аналізу загроз і каналів витоку інформації.

Тема 5. Управління ризиками інформаційної безпеки.

Управління ризиками інформаційної безпеки. Підходи до управління ризикам ІБ. Вимоги стандарту ISO/IEC 27005.

Тема 6. Система управління інформаційною безпекою «Матриця».

Теорія управління інформаційною безпекою. Система управління інформаційною безпекою «Матриця». Основні завдання СУІБ «МАТРИЦЯ». Методичні модулі СУІБ. Функціональні можливості СУІБ «МАТРИЦЯ».

Модуль 2

Змістовий модуль 3. Методи контролю та економічного обґрунтування системи захисту інформації

Тема 7. Система управління інцидентами інформаційної безпеки.

Система управління інцидентами інформаційної безпеки. Процеси реагування на інциденти. Документація системи управління інцидентами. Основи управління інцидентами інформаційної безпеки.

Тема 8. Аудит інформаційної безпеки.

Аудит інформаційної безпеки. Типи та види Аудит інформаційної безпеки. Основні етапи аудиту.

Змістовий модуль 4. Доцільність витрат на захист інформації

Тема 9. Економічне обґрунтування доцільності витрат на захист інформації.

Проблемні питання економічного обґрунтування доцільності витрат на захист інформації. Огляд існуючих методів оцінки доцільності витрат на ІБ. Метод оцінювання окупності вкладень у проекти із захисту інформації в невеликих компаніях.

Правила оцінювання

При заповненні заліково-екзаменаційної відомості та залікової книжки (індивідуального навчального плану) студента, оцінка, виставлена за 100-бальною шкалою, переводиться до державної 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**
ЗАРАХОВАНО	**Відмінно** – відмінне виконання лише з незначною кількістю помилок	90-100	A
	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 - непогано, але зі значною кількістю недоліків	69-74	D
	Достатньо – виконання задовольняє мінімальні критерії	60-68	E
НЕЗАРАХОВАНО	**Незадовільно** – потрібно попрацювати перед тим як отримати залік або екзамен (без повторного вивчення модуля)	35-59	FX
	Незадовільно - необхідна серйозна подальша робота (повторне вивчення модуля)	<35	F

Лабораторні заняття

Оцінюються за ступенем залученості (до 15 балів) та виконання завдання (до 15 балів). Ступінь залученості визначається рівнем виконання завдань самостійної роботи. Максимальна сума становить 30 балів.

Практичні заняття

Оцінюються за ступенем залученості (до 15 балів) та виконання завдання (до 15 балів). Ступінь залученості визначається рівнем виконання завдань самостійної роботи. Максимальна сума становить 30 балів.

Модульний контроль

Оцінюються за вірними відповідями на тестові модульні питання (15 питань в тесті). Максимальна кількість становить 40 балів за модуль.

Залік

Підсумковий контроль знань здійснюється шляхом обчислення середньоарифметичної суми балів двох модульних оцінок за 100-бальною шкалою.

Результати навчання

1. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
2. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами;
3. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

Команда викладачів:

Лисечко Володимир Петрович (http://kart.edu.ua/pro-kafedry-tz-ua/kolectuv-kafedru-tz-ua/lusechko-vp-ua) – лектор з напрямних систем електричного та оптичного зв'язку в УкрДУЗТ. Отримав ступінь к.т.н. за спеціальністю 05.12.02 телекомунікаційні системи та мережі в УкрДАЗТ у 2007 році. Напрямки наукової діяльності: методи обробки інформації у телекомунікаційних системах та мережах, інфокомунакаційних системах залізничного транспорту.

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/