Український державний університет залізничного транспорту

Рекомендовано
на засіданні кафедри
транспортного зв'язку
прот. № 1 від 30.08.2024 р.

СИЛАБУС З ДИСЦИПЛІНИ

ЗАХИСТ МЕРЕЖЕВИХ СИСТЕМ

Освітній рівень перший (бакалавр)

Галузь знань 17 Електроніка, автоматизація та електронні комунікації

Спеціальність 172 Телекомунікації та радіотехніка

Освітня програма Телекомунікації та радіотехніка

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

Команда викладачів:

Лектор: Індик Сергій Володимирович (к. т. н., доцент кафедри транспортного зв'язку), Контакти: +38 (057) 730-10-81, e-mail: serhii.indyk@kart.edu.ua
Асистент лектора: Мазіашвілі Артур Рамазійович (асистент), Контакти: +38 (057) 730-10-81, e-mail: maziashvili@kart.edu.ua Години прийому та консультації: вівторок з 14.10-15.30
Веб сторінка курсу: http://do.kart.edu.ua/ Додаткові інформаційні матеріали: http://metod.kart.edu.ua

Харків – 2024

Анотація курсу

Завданням дисципліни є навчання студентів побудуванню аналітичних моделей порушників, оцінки їх можливостей та інтерпретації результатів аналізу і оцінки ризиків безпеки, застосування методів системного аналізу у вирішенні задач захисту інформації. Вивчення студентами сучасних методів побудови безпечних систем, що відповідають вимогам провідних міжнародних стандартів. Студент буде вміти розробляти вимоги та обирати для впровадження заходи захисту інформації; вибирати та застосовувати критерії та показники оцінки рівня захищеності; розробляти функціональні моделі процесів захисту інформації, організовувати діяльність персоналу згідно вимог ISO/IEC 27001; розробляти моделі загроз безпеці інформації; розробляти та верифікувати профілі захисту інформації згідно вимог НД ТЗІ; оцінювати ризики безпеки згідно вимог ISO/IEC 27005; застосовувати стандартні пакети при розв'язанні прикладних задач моделювання процесів захисту інформації.

Чому ви маєте обрати цей курс?

Вивчивши курс студент буде обізнаним з факторами та каналами уразливості інформації, основними методами, принципами, способами, алгоритмами та протоколами захисту інформації; критеріями та показниками оцінки якості захисту інформації; методами оцінювання та аналізу загроз та ризиків безпеки; основними протиріччями, проблемами, тенденціями та напрямами розвитку теорії та практики захисту інформації, прогнозування їх можливостей та можливостей порушників; функціональними можливостями та порядком застосування сучасних методів аналізу ризиків безпеки; методами оцінки ефективності систем управління інформаційною безпекою.

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

Огляд курсу

Цей курс, який вивчається протягом другого семестру, дає студентам глибоке розуміння в розробці та пропонуванні нових технічних рішень та застосовувань нових технологій у сфері безпеки телекомунікаційних систем та мереж.

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

Схема курсу

<table>
<tr><td rowspan="8">Поміркуй</td><td>Лекції</td><td></td></tr>
<tr><td>Матеріал для самостійної роботи</td><td></td></tr>
<tr><td>Обговорення на заняттях</td><td rowspan="7">Виконай</td></tr>
<tr><td>Лабораторні заняття</td></tr>
<tr><td>Практичні заняття</td></tr>
<tr><td>Індивідуальні консультації</td></tr>
<tr><td>Консультації</td></tr>
<tr><td>Залік</td></tr>
</table>

Лабораторні та практичні заняття курсу передбачають виконання завдань щодо оцінки критичності інформаційних ресурсів, дослідження функціональних можливостей спеціалізованого програмного забезпечення, програмній реалізації виявлення мережевих атак, оцінку ефективності систем захисту інформації.

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 відбуваються процеси безпеки телекомунікаційних систем та мереж. Ви повинні бути готовими до дискусій та мозкових штурмів – ми хочемо знати, що Ви думаєте!

Приклади питань для обговорення на заняттях:

1) Що таке ARP-SPOOFING атака?

2) Назвіть засоби перегляду мережевого трафіку.

3) На основі яких стандартів відбувається оцінка критичності інформаційних ресурсів телекомунікаційної мережі?

Теми курсу

Тема 1. Основні поняття та визначення інформаційної безпеки. Структура інформаційної безпеки.

Тема 2. Загальні положення щодо захисту від несанкціонованого доступу.

Тема 3. Класифікація загроз інформації. Несанкціонований доступ до комп'ютерних систем.

Тема 4. Оцінка вразливостей інформаційних ресурсів. Окремі моделі загрози та порушника.

Тема 5. Класифікація типових віддалених атак.

Тема 6. Загрози інформації стека TCP IP. Комп'ютерні віруси.

Тема 7. Класифікація каналів витоку інформації.

Тема 8. Методи та засоби захисту від витоку інформації.

Лабораторні заняття

Оцінка критичності інформаційних ресурсів на основі вимог стандарту NIST SP 800-60.

Дослідження функціональних можливостей програмного забезпечення Wireshark.

Програмне логування мережевих пакетів в файл.

Використання Wireshark для перегляду мережного трафіку.

Використання Wireshark для дослідження кадрів Ethernet.

Використання Wireshark для дослідження пакетів протоколу IP.

Дослідження динамічного управління ризиками.

Програмна реалізація виявлення заданої мережевої атаки, автоматичне реагування і логування підозрілої активності.

Оцінка ефективності систем захисту інформації.

Виявлення ARP-SPOOFING атаки.

Практичні заняття

Дослідження автентичності змісту зашифрованих файлів за допомогою вбудованих функцій MS Windows.

Дослідження автентичності змісту зашифрованих файлів за допомогою спеціалізованого програмного забезпечення.

Дослідження процесів криптографічного захисту електронних даних. Цифровий електронний підпис.

Оцінка ефективності систем захисту інформації.

Вимоги викладача

Система вимог та правил поведінки студентів на заняттях, рекомендації щодо виконання контрольних заходів, присутність на заняттях та академічна активність, що гарантують високу ефективність навчального процесу і є обов'язковою для студента, визначаються Положенням про організацію освітнього процесу в УкрДУЗТ.

Зокрема студенти повинні виконувати вимоги з охорони праці, техніки безпеки, виробничої санітарії, протипожежної безпеки, передбачені відповідними правилами та інструкціями; самостійно виконувати навчальні завдання, завдання поточного та підсумкового контролю результатів навчання; відвідувати заняття відповідно до розкладу занять або індивідуального графіку.

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**
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 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.

Курсовий проект

Підсумковий контроль знань здійснюється шляхом усного опитування за 100-бальною шкалою.

Модульний контроль

Оцінюються за вірними відповідями на тестові модульні питання (20 питань в тесті). Максимальна кількість становить 40 балів за модуль.

Екзамен

Підсумковий контроль знань здійснюється шляхом обчислення середньоарифметичної суми балів двох модульних оцінок за 100-бальною шкалою (без складання екзамену) або проведження екзамену шляхом комп'ютерного тестування або відповідей на питання екзаменаційних білетів.

Команда викладачів:

Індик Сергій Володимирович (https://kart.edu.ua/staff/indyk-sv) –лектор в УкрДУЗТ. Отримав ступінь к.т.н. за спеціальністю 05.12.02 телекомунікаційні системи та мережі в УкрДУЗТ в 2021 році. Напрямки наукової діяльності: обробка інформації у телекомунікаційних системах та мережах.

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/

Інформаційні матеріали

1. Лістровий С.В. Інформаційно-управляючі системи та організації паралельних обчислень / С. В. Лістровий, О. С. Лістрова, М. А. Мірошник; за ред. С. В. Лістрового. Х. : УкрДУЗТ ; Діса плюс, 2015.

2. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. - К.: ДУТ, 2015. - 288 с.

3. http://www.e-helper.com.ua/node/120

4. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

5. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкційованого доступу.

6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкційованого доступу.

7. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкційованого доступу.

8. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкційованого доступу.

9. НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкційованого доступу.

10. ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements.

11. ISO/IEC 27002:2007 Information technology — Security techniques — Code of practice for information security management.