Український державний університет залізничного транспорту

Затверджено
рішенням вченої ради факультету
інформаційно-керуючих систем та
технологій
прот. № 1 від 29.08.2019 р.

Рекомендовано
на засіданні кафедри
транспортного зв'язку
прот. № 1 від 27.08.2018 р.

СИЛАБУС З ДИСЦИПЛІНИ

БЕЗПЕКА ТА КЕРУВАННЯ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

I, II семестр 2019-2020 навчального року

Освітній рівень другий (магістерський)

Галузь знань 27 Транспорт

Спеціальність 273 Залізничний транспорт

Освітня програма Інфокомунікації та інженерія

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

Команда викладачів:

Лектор: Сєвєрінов Олександр Васильович (кандидат технічних наук, доцент), 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

1. 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.

Цілями та завданнями навчальної дисципліни є набуття студентами:

1) знань, що визначаються змістовними модулями навчальної дисципліни, згрупованими у такі блоки:

- фактори та канали уразливості інформації, основні методи, принципи, способи, алгоритми та протоколи захисту інформації;
- критерії та показники оцінки якості захисту інформації;
- методи оцінювання та аналізу загроз та ризиків безпеки;
- основні протиріччя, проблеми, тенденції та напрями розвитку теорії та практики захисту інформації, прогнозування їх можливостей та можливостей порушників;
- функціональні можливості та порядок застосування сучасних методів аналізу ризиків безпеки;
- методи оцінки ефективності систем управління інформаційною безпекою.

2) умінь:

- 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.

2. Мета курсу

Цей курс формує базові знання з проблем теорії та практики захисту інформації, в ньому розглядаються основні протиріччя забезпечення безпеки інформації та методи їх вирішення. Дисципліна має на меті сформувати та розвинути в студентів основні компетенції, до яких відносяться:

знання та робота із основними методами, принципами, способами керування інформаційною безпекою;

здатність враховувати можливі впливи порушників та прогнозування розвитку методів порушення безпеки інформації.

3. Організація навчання

3.1. Опис навчальної дисципліни

Кількість кредитів – 7.

Загальна кількість годин вивчення дисципліни – 210.

Кількість годин відведена на проведення лекцій – 70.

Кількість годин відведена на проведення лабораторних занять – 35.

Кількість годин відведена на самостійну роботу – 105.

Рік та курс навчання – 2019/20 рік, 1 курс.

Термін викладання – 2 семестри.

3.2. Теми курсу за модулями

Вступна лекція

Основні поняття та визначення інформаційної безпеки.

Проблеми захисту інформації від несанкціонованого доступу.

Нормативно-правове забезпечення інформаційної безпеки.

Визначення інформації, що підлягає захисту.

Загальні положення щодо захисту від НСД.

Нормативно-правові документи нижнього рівня.

Захист державної таємниці.

Загрози і канали витоку інформації.

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 об'єктів ІС

Загрози для механізмів керування системою захисту.

Керування ризиками інформаційної безпеки.

Підходи до управління ризикам ІБ. Вимоги стандарту ISO/IEC 27005.

Теорія управління інформаційною безпекою.

Система управління інформаційною безпекою «Матриця».

Методичні модулі СУІБ.

Система керування інцидентами інформаційної безпеки.

Документація системи керування інцидентами.

Процеси реагування на інциденти.

Основи керування інцидентами інформаційної безпеки.

Аудит інформаційної безпеки.

Основні етапи аудиту інформаційної безпеки.

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.

Підсумкова лекція

Теми лабораторних занять.

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

Дослідження можливостей програмного комплексу Digital Security Office 2006.

Оцінка і аналіз ризиків за допомогою системи управління інформаційною безпекою «Матриця».

Оцінка ефективності систем захисту інформації.

Програмне логування мережевих пакетів в файл.

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

Вивчення функціональних можливостей програми ETTERCAP.

Виявлення ARP-SPOOFING атаки.

3.4. 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. Автоматизація виробничих процесів / І. В. Ельперін, О. М. Пупена, В. М. Сідлецький, С. М. Швед − К. : Ліра-К., 2015.

3. Матвієнко, М. П. Комп'ютерна логіка / М. П. Матвієнко. - К. : Ліра-К, 2015.

4. Матвієнко, М. П. Пристрої цифрової електроніки / М. П. Матвієнко К. : Ліра-К, 2015.

8. http://metod.kart.edu.ua/

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

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

11. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

12. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

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

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

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

16. ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements.

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

18. ISO/IEC 27005:2008 Technologies de l'information — Techniques de sécurité − Gestion du risque en sécurité de l'information.

19. В.В. Домарев, Д.В. Домарев. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k), Донецьк: Велстар, 2012. – 146 с.

3.5. 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.

3.6. Порядок оцінювання результатів навчання

Контроль знань у рамках навчальної дисципліни здійснюється з урахуванням кредитно-модульної системи відповідно до Положення про контроль та оцінювання якості знань студентів в УкрДУЗТ.

Методи контролю: поточний контроль знань здійснюється під час проведення практичних та лабораторних занять шляхом опитування; модульний контроль здійснюється шляхом виконання контрольних завдань (тестів); підсумковий контроль знань здійснюється шляхом обчислення середньоарифметичної суми балів двох модульних оцінок за 100-бальною шкалою (без складання екзамену) або проводження екзамену шляхом комп'ютерного тестування або відповідей на питання екзаменаційних білетів; захист курсової роботи здійснюється перед комісією у складі науково-педагогічних працівників кафедри шляхом опитування.

Принцип формування оцінки за модуль у складі залікових кредитів I і II за 100-бальною шкалою показано у таблиці, де наведена максимальна кількість балів, яку може набрати студент за різними видами навчального навантаження.

Максимальна кількість балів за модуль		
Поточний контроль	Модульний контроль (Тести)	Сума балів за модуль
До 60	До 40	До 100
Поточний Контроль		1 семестр
Відвідування занять. Активність на заняттях (Лекціях, практичних, лабораторних).		10
Здача в строк лабораторних робіт		50
Підсумок		до 60
Поточний Контроль		2 семестр
Відвідування занять. Активність на заняттях (Лекціях, лабораторних).		10
Здача в строк лабораторних робіт		50
Підсумок		до 60

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

3.7. Кодекс академічної доброчесності

При вивченні навчальної дисципліни студенти повинні дотримуватись Кодексу академічної доброчесності УкрДУЗТ (http://kart.edu.ua/documentu-zvo-ua).

Зокрема, дотримання Кодексу академічної доброчесності УкрДУЗТ означає, що усі види робіт 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 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.

3.8. 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 УкрДУЗТ 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/