Національний університет «Полтавська політехніка імені Юрія Кондратюка»

Силабус навчальної дисципліни

«Методи та алгоритми захисту дискретної інформації»

Спеціальність	*172 - Електронні комунікації та радіотехніка*
Освітня програма	*Телекомунікаційні системи та мережі*
Освітній рівень	*Другий (магістерський)*
Статус дисципліни	*Обов'язкова*
Мова викладання	*Українська*
Курс / семестр	*1 курс, 1 семестр*
Кількість кредитів ЄКТС	5
Розподіл за видами занять та годинами навчання	*Лекції - 28 год.*
	Лабораторні - 22 год.
	Курсова робота - 30 год.
	Самостійна робота - 70 год.
Форма підсумкового контролю	*Екзамен – 1 семестр*
Кафедра	*Кафедра автоматики, електроніки та телекомунікацій, ауд. 314Ф, https://nupp.edu.ua/page/kafedra-avtomatiki-yelektroniki-ta-telekomunikatsiy.html*
Викладач (-і)	*Фомін Олександр Сергійович, к.т.н., доцент*
Контактна інформація викладача	*olexandr.fomin@nupp.edu.ua*
Дні занять	*За розкладом, відповідно до графіку навчального процесу*
Консультації	*Аудиторія 314Ф відповідно до графіку*

Мета навчальної дисципліни – *формування знань і вмінь студентів щодо принципів функціонування та характеристик мережевих служб дискретної інформації, принципів, методів та алгоритмів захисту дискретної інформації при побудові та експлуатації телекомунікаційної інфраструктури.*

Програмні результати навчання

ПР 2 – Використовувати принципи та концепції побудови телекомунікаційних систем та мереж у поєднанні з потребіним математичним апаратом.
ПР 4 – Застосовувати сучасні ІТ в професійній діяльності.
ПР 7 – Організовувати захист інформації в інфокомунікаційних мережах, здійснювати адміністрування інфокомунікаційних мереж, впроваджувати, налагоджувати та адмініструвати мережеве та інше системне програмне забезпечення.
ПР 12 – Застосовувати знання вимог законодавчої бази стосовно особливостей інформаційної безпеки на підприємствах інноваційної діяльності; базових моделей керування доступом; видів та механізмів контролю рівня безпеки.

Передумови для навчання

Попередньо опанована дисципліна: «Вища математика».

Індивідуальне завдання	*Курсова робота*

Зміст навчальної дисципліни

Тема 1. Основи поняття теорії інформації та криптографії. Модель системи з криптозахистом. Класифікація криптосистем. Методи криптоаналіза і типи атак. Мінімальні довжини ключів. **Тема 2. Історія розвитку криптографічних методів захисту дискретної інформації.** Способи приховування інформації у стародавні часи. Криптографія середньовіччя. Становлення криптографії як науки у XX столітті. **Тема 3. Класичні шифри.** Моноалфавітні шифри. Біграмні шифри заміни. Поліграмний шифр заміни Хіл-Ла. Шифр гамування Віженера. Криптоаналіз поліалфавітних шифрів. **Тема 4. Досконала криптостійкість інформаційних систем.** Визначення та умови досконалої криптостійкості. Криптосистема Вернама. Відстань єдиності. **Тема 5. Блокові шифри.** Вступ та класифікація. SP-мережі. Проект «Люцифер». Комірка Фейстеля. Шифр DES. Стандарт шифрування США AES. **Тема 6. Генератори псевдовипадкових чисел.** Лінійний конгруентний генератор. Регістр

зсуву з лінійним зворотним зв'язком. Криптографічно стійкі генератори псевдовипадкових чисел. **Тема 7. Потокові шифри.** Визначення потокового шифру та способи реалізації. Шифр RC4. **Тема 8. Криптографічні хеш-функції.** Імітовставлення. Колізії у хеш-функціях. Ймовірність колізії. Комбінації хеш-функцій. **Тема 9. Асиметричні криптосистеми.** Криптосистема RSA. Криптосистема Ель-Гамаля. Еліптичні криві. Довжини ключів. Інфраструктура відкритих ключів. **Тема 10. Розповсюдження ключів.** Поділ секрету. Триетапний протокол Шаміра на комутативних шифрах. Симетричні протоколи. Асиметричні протоколи. Порогові схеми. Розподіл секрета по коаліціях. **Тема 11. Стеганографія.** Основні терміни та визначення. Історичні приклади стеганосистем Математична мо-дель та структурна схема стеганографічної системи. Класифікація контейнерів. **Тема 12. Реалізація систем захисту дискретної інформації.** Система Kerberos для локальної мережі. Pretty Good Privacy. Протокол SSL/TLS. За-хист IPsec на мережному рівні. **Тема 13. Автентифікація користувачів.** Багатофакторна автентифікація. Ентропія та криптостійкість паролів. Аутентифікація за паролем. Зберігання паролів та автентифікація в ОС. Аутентифікація у веб-сервісах. **Тема 14. Програмні вразливості.** Контроль доступу до інформаційних систем. Контроль доступу в ОС. Види програмних уразливостей. Міжсайтовий скриптинг. SQL-ін'єкції з виконанням коду базою даних інтернет-сервісу.

Сторінка курсу на платформі Moodle	https://dist.nupp.edu.ua/course/view.php?id=6145

Рекомендовані джерела

Базова

1. Богуш В.М., Бровко В.Д., Кобус О.С., В.Д. Козюра В.Д. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. - Київ: Ліра-К, 2023. - 483 с.
2. Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. Основи кіберпростору, кібер-безпеки та кіберзахисту - Київ : Ліра-К, 2024. - 554 с.
3. Присяжнюк М.М., Рідей Н.М., Титова Н.М. Інформаційна безпека та кібербезпека держави. Навчальний посібник - Ліра-К, 2024. - 224 с.

Допоміжна

1. Мельник І., Лунтовський А. Проектування та дослідження комп'ютерних мереж. – Київ: Університет «Україна», 2010. – 362 с.
2. Мельник І., Лунтовський А. Комп'ютерні мережі та телекомунікації. – Київ: Університет «Україна», 2007. – 274 с.
3. Blum R., Bresnahan C. Linux command line and shell scripting bible. – Wiley, 2021. – 832 p.
4. Шульга В. П.,Іванченко Є. В., Вишневська Н. С., Бербер А. С. Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. Сучасний захист інформації, 2024 р., 3(59) - 6-19 с.
5. Гаврилова А. А., Король О. Г., Воропай Н. І., Севрюкова Є. О., Бондаренко К. О. Аналіз методів криптографічної автентифікації та виявлення маніпуляцій для великих даних. Сучасний захист інформації, 2024 р., 1(57) - 97-102 с.
6. Laptiev, O., Tkachev, V., Maystrov, O., Krasikov, O., Open'ko, P., Khoroshko, V., Parkhuts, L.The method of spectral analysis of the determination of random digital signals. International Journal of Communication Networks and Information Security (IJCNIS). Vol 13, No 2, August 2021 P.271-277. ISSN: 2073-607X (Online). DOI:10.54039/ijcnis.v13i2.5008 https://www.ijcnis.org/index.php/ijcnis/article/view/5008.
7. Sarkar, S., Almukaynizi, M., Shakarian, J., & Shakarian, P. (2019). Predicting enterprise cyber incidents using social network analysis on dark web hacker forums. The Cyber Defense Review, 87–102. https://www.jstor.org/stable/26846122.
8. Florian Klaus Kaisera, Tobias Budiga, Elisabeth Goebela, Tessa Fischera, Jurek Muffa, Marcus Wiensa and Frank Schultmanna. Attack Forecast and Prediction. C&ESAR'21: Computer Electronics Security Application Rendezvous, November 16-17, 2021, Rennes, France.
9. Jones, M., Kotsalis, G., Shamma, J.S. (2013). Cyber Attack Forecast Modeling and Complexity Reduction Using a Game-Theoretic Framework. In: Tarraf, D. (eds) Control of Cyber-Physical Systems. Lecture Notes in Control and Information Sciences, vol 449. Springer, Heidelberg. https://doi.org/10.1007/978-3-319-01159-2_4.

10. Ganjali, A., Marwat, S. S., & Sifalakis, M. (2012). Critical infrastructure protection: A mathematical modeling perspective. Journal of Network and Systems Management, 20(1), 128-144.

Система оцінювання результатів навчання

За результатами поточного контролю протягом семестру студент може отримати максимально 50 балів, за результатами підсумкового контролю 50 балів. Студент, який повністю виконав програму навчальної дисципліни і отримав достатню рейтингову оцінку (не менше 25 балів), допускається до підсумкового контролю з дисципліни.

Більш детальна інформація щодо оцінювання наведена в робочій навчальні програмі

Накопичування балів з навчальної дисципліни

Види навчальної роботи	**Max кількість балів**
Робота на заняттях та виконання лабораторних робіт	50
Екзамен	50
Максимальна кількість балів	**100**

Курсова робота оцінюється за окремою 100-бальною шкалою.

Пояснювальна записка	**Захист роботи**	**Сума**
50	50	**100**

Відповідність шкали оцінювання ЄКТС національній системі оцінювання та шкалі оцінювання Національного університету «Полтавська політехніка імені Юрія Кондратюка»

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою
90 - 100	A	відмінно
82 - 89	B	добре
74 - 81	C	
64 - 73	D	задовільно
60 - 63	E	
35 - 59	FX	незадовільно
1 - 34	F	

Політика навчальної дисципліни

Вивчення навчальної дисципліни потребує роботи з інформаційними джерелами, підготовки до лекцій і лабораторних робіт, виконання усіх завдань згідно з навчальним планом.

Підготовка до лабораторних робіт передбачає: ознайомлення з питаннями, які виносяться заняття з відповідної теми; вивчення лекційного матеріалу. Виконання лабораторних робіт повинно демонструвати ознаки самостійності виконання здобувачем такої роботи, відсутність ознак повторюваності та плагіату.

Присутність здобувачів вищої освіти на лабораторних і лекційних заняттях є обов'язковою, важливою також є їх участь в обговоренні всіх питань теми. Пропущені заняття мають бути відпрацьовані. Здобувач вищої освіти повинен дотримуватися навчальної етики, поважно ставитися до учасників процесу навчання, дотримуватися дисципліни й часових (строкових) параметрів навчального процесу.

Більш детальну інформацію щодо компетентностей, результатів навчання, методів навчання, форм оцінювання, самостійної роботи наведено у робочій програмі навчальної дисципліни https://dist.nupp.edu.ua/course/view.php?id=6145

Силабус затверджено на засіданні кафедри «Автоматики, електроніки та телекомунікацій»
«19» серпня 2024 р. Протокол № 1