



Силабус курсу

«Системне адміністрування та безпека інформаційних і комунікаційних систем»

Ступінь вищої освіти – магістр

Галузь знань: 01 Освіта/Педагогіка

Спеціальність: 015 Професійна освіта (Цифрові технології)

Освітньо-наукова програма: Професійна освіта (Комп'ютерні технології)»

Дні занять: вівторок, четвер, 9.20-12.30, ауд. 216

Консультації: понеділок 14.05, ауд. 216

Рік навчання: 2, Семестр: IV

Компонент освітньо-наукової програми: вибіркова навчальна дисципліна

Кількість кредитів: 5 Мова викладання: українська

Керівник курсу

кандидат технічних наук, доцент, **Франко Юрій Павлович**

Контактна інформація

franko@tnpu.edu.ua; +380672568938

Опис дисципліни

Дисципліна «Системне адміністрування та безпека інформаційних і комунікаційних систем» призначена для підготовки магістрів у галузі сучасних комунікаційних систем. Даний курс дозволяє набути теоретичні знання з управління ресурсами обчислювальних систем, здобути практичні навички з системного адміністрування та передбачає в умовах зростаючої інформатизації суспільства підвищення рівня безпеки захисту інформаційно-комунікаційних систем.

Мета вивчення дисципліни полягає у формуванні у майбутніх фахівців умінь та компетенцій для управління системними ресурсами комп'ютерів та комп'ютерних мереж; здобутті базових навичок практичної роботи в якості системного адміністратора; виявлення технічних каналів витоку інформації, шляхів деструктивного впливу на інформацію та засоби її обробки; застосуванні заходів та засобів, спрямованих на технічний захист інформації на об'єктах інформаційної діяльності.

Організація навчання (структура курсу)

Години (лек. / лаб. роб.)	Тема	Результати навчання	Завдання
	Змістовий модуль 1. Системне адміністрування комп'ютерів і комп'ютерних мереж.		
2 / 2	1. Стратегія та методика адміністрування.	Знати основні методи адміністрування, налагодження, оптимізації мережевих служб; основні види, характеристики та функціональні можливості сучасних мережевих служб. Вміти адмініструвати, налаштовувати сучасні серверні технології; відлагоджувати та усувати конфлікти в сучасних мережевих службах та серверах.	Завдання до лаб.роботи, питання, тести
2 / 4	2. Основні відомості про інфраструктуру мережі. Створення мереж Windows на основі стандартних компонентів.	Знати основні методи тестування серверних технологій, визначення неполадок та методи їх усунення; основні тенденції розвитку комп'ютерних мереж та мережевих протоколів, служб та серверів. Вміти здійснювати сервісне обслуговування мережевих серверних технологій; проводити постійне оновлення та вдосконалення програмного та апаратного забезпечення комп'ютерних систем та мереж у відповідності із сучасними вимогами та тенденціями.	Завдання до лаб.роботи, питання, тести
2 / 4	3. Адміністрування домену Active directory	Знати основні методи адміністрування, налагодження, оптимізації мережевих служб; основні методи тестування серверних технологій, визначення неполадок та методи їх усунення. Вміти адмініструвати домен Active directory, налаштовувати сучасні серверні технології структуру розподілених обчислювальних систем та комп'ютерних мереж.	Завдання до лаб.роботи, питання, тести
2 / 4	4. Основи роботи системи для серверів.	Знати основні види, характеристики та функціональні можливості сучасних мережевих служб; принципи функціонування та алгоритми роботи мережевих протоколів; основні стандарти протоколів; налагодження, оптимізації мережевих служб; основні методи	Завдання до лаб.роботи, питання, тести

		тестування серверних технологій, визначення неполадок та методи їх усунення. Вміти адмініструвати, налаштовувати сучасні серверні технології; відлагоджувати та усувати конфлікти в сучасних мережевих службах та серверах; здійснювати сервісне обслуговування мережевих серверних технологій;	
	Змістовий модуль 2. Технологія управління системними ресурсами		
1 / 4	5. Засоби побудови захищених комп'ютерних мереж	Вивчити методи побудови захищених комп'ютерних систем та мереж; можливі технічні канали витоку інформації. Вміти планувати та організовувати свою роботу та роботу підрозділу з урахуванням вимог до захисту інформації з обмеженим доступом.	Завдання до лаб.роботи, питання, тести
1 / 4	6. Основи web-хостингу	Вивчити використання web-сервера, програмних засобів реалізації web-сервера. Вміти налаштовувати основні функції Apache, підтримку захищених web-вузлів, організовувати віртуальні домени.	Завдання до лаб.роботи, питання, тести, ІНДЗ
2 / 4	7. Системне та мережеве адміністрування	Огляд засобів системного та мережевого адміністрування. Вміти застосовувати систему моніторингу Інтернет сервісів, моделювання і моніторинг діяльності, керувати на основі Service Level Agreement.	Завдання до лаб.роботи, питання, тести
	Змістовий модуль 3. Захист інформації у автоматизованих системах, телекомунікаційних мережах та відкритих мережах зв'язку.		
2 / 2	8. Концептуальні засади забезпечення інформаційної безпеки України	Ознайомитися з нормативно-правовим забезпеченням захисту інформації в інформаційно-комунікаційних системах.	Завдання до лаб.роботи, питання, тести
2 / 2	9. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації	Знати основні поняття, терміни та визначення технічного захисту інформації. Знати основні загрози безпеки автоматизованих систем обробки інформації. Вміти застосовувати забезпечення безпеки автоматизованих систем обробки інформації.	Завдання до лаб.роботи, питання, тести, ІНДЗ

2 / 4	10. Методи та засоби блокування технічних каналів витоку інформації	Вміти застосовувати: методи пасивного та активного захисту інформації, методи та засоби захисту акустичної інформації, методи та засоби захисту електромагнітної інформації, методи захисту від ВЧ-нав'язування, методики і засоби пошуку радіозакладних пристроїв.	Завдання до лаб.роботи, питання, тести, ІНДЗ
1 / 4	11. Методи захисту інформації у автоматизованих системах	Знати застосовування розмежування доступу до інформації в залежності від повноважень користувача. Вміти використовувати паролі, проводити захист інформації у комп'ютерах від вірусів, шифрувати інформацію у комп'ютерах при її зберіганні.	Завдання до лаб.роботи, питання, тести, ІНДЗ
1 / 2	12. Методи захисту інформації у телекомунікаційних мережах та відкритих каналах зв'язку	Знати стеганографічні методи захисту письмової інформації. Вміти застосовувати на практиці симетричні та асиметричні алгоритми шифрування інформації.	Завдання до лаб.роботи, питання, тести, ІНДЗ

Формування програмних компетентностей

Індекс в матриці ОП	Програмні компетентності
Інтегральна компетентність	Здатність розв'язувати складні задачі і проблеми в освітній та виробничій галузях професійної діяльності згідно спеціалізації, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.
ЗК 6	Здатність до розробки й застосування програмного забезпечення виробничого або освітнього процесів.
ФК 13	Здатність студентів опанувати принципи побудови комплексних систем захисту інформації, розробки, дослідженню та застосуванню механізмів захисту інформації.
ФК15	Здатність до адміністрування і налаштування сучасних інформаційних і комунікаційних систем із врахуванням фактору захисту інформації.
ПРН 17	Відлагоджувати та усувати конфлікти в сучасних мережевих службах та серверах; здійснювати сервісне обслуговування мережевих серверних технологій; виконувати моніторинг безпеки комп'ютерних мереж та будувати захищені комп'ютерні системи.
ПРН 18	Володіти основними методами адміністрування, налагодження, оптимізації мережевих служб; методикою моніторингу безпеки комп'ютерних мереж та технологією побудови захищених комп'ютерних систем.

Літературні джерела

1. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник в 2-х т. / В.В. Поповский, А.В. Персиков. – Харьков: ООО «Компания СМИТ», 2006. – 238 с.
2. Рибальський О.В. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України / О.В. Рибальський, В.М. Смаглюк, В.Г. Хахановський – К.: НАВС, 2013. – 255 с.
3. Рибальський О.В. Основи інформаційної безпеки та технічного захисту інформації. Навчальний посібник для курсантів ВНЗ МВС України / О.В. Рибальський, В.Г. Хахановський, В.А. Кудінов. – К.: Вид. Національної академії внутріш. справ, 2013. – 104 с.
4. Браїловський М.М. Захист інформації у банківській діяльності / М.М. Браїловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ «ПоліграфКонсалтинг», 2004. – 216 с.
5. Ленков С.В. Методы и средства защиты информации. В 2-х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко.– Под ред. В.А. Хорошко.–К.: Арий, 2008. – Том 1. Несанкционированное получение информации. – 464 с.
6. Ленков С.В. Методы и средства защиты информации. В 2-х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – Под ред. В.А. Хорошко. – К.: Арий, 2008. – Том 2. Информационная безопасность. – 344 с.
7. URL: http://www.zhu.edu.ua/mk_school/mod/page/view.php?id=3333&lang=ru
8. Інформаційні ресурси та сервіси в інфокомунікаціях. URL: <http://www.dut.edu.ua/ua/1430-informatsiyni-resursi-ta-servisi-v-infokomunikatsiyah>
9. Комп'ютерна мережа. URL: https://uk.wikipedia.org/wiki/Комп%27ютерна_мережа
10. Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах. URL: <https://zakon.rada.gov.ua/laws/show/z0027-02#Text>
11. Закон України Про захист інформації в інформаційно-телекомунікаційних системах. URL: <https://ips.ligazakon.net/document/Z008000>
12. Забезпечення захисту інформації в системі. URL: https://protocol.ua/ua/pro_zahist_informatsii_v_informatsiyno_telekomunikatsiynih_sistemah_statiya_9/
13. Закон України Про криптографічний та технічний захист інформації URL: <https://ips.ligazakon.net/document/NT1819>

Політика дисципліни

- **Політика щодо дедлайнів та перескладання:** Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності балів). Перескладання модулів відбувається із дозволу навчально-методичного відділу за наявності поважних причин.
- **Політика щодо академічної доброчесності:** Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки до заняття.
- **Політика щодо відвідування:** Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

Остаточна оцінка за курс розраховується наступним чином:

Види оцінювання	% від сумарної оцінки
Модуль 1 (теми 1-4) усне опитування, тести, завдання	20
Модуль 2 (теми 5-7) усне опитування, тести, завдання	15
Модуль 3 (теми 8-12) усне опитування, тести, завдання	25
ІНДЗ	15
Підсумковий контроль (теми 1-12) – тести, завдання	25
Всього	100

Шкала оцінювання студентів:

ECTS	Бали	Зміст
A	90-100	відмінно
B	85-89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом

Пререквізити

Ефективність засвоєння змісту дисципліни значно підвищиться, якщо студент попередньо опанував базові знання інформаційних технологій.

Знання з побудови, керування, модернізації, комп'ютерних мереж та захисту інформації можуть бути використані для розробки комплексних систем технічного захисту інформації.

Формат дисципліни

Змішаний (blended) – дисципліна має супровід в системі Moodle, структуру, контент, завдання і систему оцінювання. Blended Learning – викладання курсу передбачає поєднання традиційних форм аудиторного навчання з елементами електронного навчання, в якому використовуються спеціальні інформаційні технології, інтерактивні елементи, онлайн консультування і т.п.

До силябусу також готуються матеріали навчально-методичного забезпечення:

- навчальний контент (розширений план лекцій, презентації, відео);
- тематика та інструкції до лабораторних робіт, ІНДЗ;
- завдання для підсумкового контролю (тести);
- електронне навчання в системі Moodle, Zoom, Google Meet.