

Силабус курсу

Системне адміністрування та безпека інформаційних і комунікаційних систем

Освітній ступінь – магістр

Галузь знань: 01 Освіта/Педагогіка

Спеціальність: 015 Професійна освіта

Спеціалізація: 015.39 Цифрові технології

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

Кількість кредитів – 5

Рік підготовки, семестр – 2 рік, 4 семестр

Компонент освітньої програми: вибірковий, професійна підготовка

Дні занять: за розкладом, авд. 216

Консультації: за розкладом, авд. 216

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 / 4	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 тестування серверних технологій, визначення неполадок та методи їх усунення. Вміти адмініструвати, налаштовувати	Завдання до лаб.роботи, питання, тести

		сучасні серверні технології; відлагоджувати та усувати конфлікти в сучасних мережеских службах та серверах; здійснювати сервісне обслуговування мережеских серверних технологій;	
	Змістовий модуль 2. Технологія управління системними ресурсами		
2 / 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
2 / 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 / 4	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

2 / 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
2 / 4	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
ЗК10	Здатність до проектування інноваційних технологій навчання і виховання майбутніх фахівців у залежності від поставлених цілей, розробки стратегічної і тактичної програм упровадження новацій у власну діяльність, а також проведення їхньої експертизи.
ФК11	Здатність до розробки й застосування програмного забезпечення виробничого або освітньо-наукового процесів.
ФК5	Здатність розробляти і реалізовувати проекти у професійній освіті, у тому числі міждисциплінарні, здійснювати їх інформаційне, методичне, матеріальне, фінансове та кадрове забезпечення.
ФК12	Здатність до розробки, тестування програмного забезпечення, адміністрування і налаштування інформаційних систем та їх інтеграції у науково-педагогічні дослідження.
ПРН2	Ефективно використовувати сучасні цифрові інструменти, інформаційні технології та ресурси у професійній, інноваційній та/або дослідницькій діяльності.
ПРН15	Уміти моделювати та здійснювати навчання згідно технологій дистанційного та змішаного навчання, враховуючи їх структурні елементи, управляти процесом у системі «викладач-студент», використовувати інструментальні програмні засоби створення мультимедійних дистанційних курсів.
ПРН18	Вміти відлагоджувати та усувати конфлікти в сучасних мережевих системах на основі використання Open-source технологій; виконувати моніторинг безпеки інформаційних систем та проектувати захищені комп'ютерні системи.

Літературні джерела

1. Гуз А. М., Довгань О. Д., Марущак А.І. Організація захисту інформації з обмеженим доступом. К.: Наук.-вид. відділ НА СБ України, 2015. 378 с.
2. Демида Б. А., Обельовська К. М., Яковина В. С. Основи адміністрування LAN у середовищі MS Windows. Навчальний посібник. Львів: Видавництво Львівської політехніки, 2013. 488 с.
3. Жадаев А. Г. Как защитись компьютер на 100%. Сбои, ошибки, вирусы СПб.: Питер, 2018. 304 с.
4. Zadiraka V. Computer Technologies in Information Security: [monograph] / V.Zadiraka, Ya. Nykolaichuk, Yu. Franko. Ternopil: «Kart-blansh», 2015. 387p.
5. Закер Крейг, Официальный учебный курс Microsoft: Управление и поддержка Microsoft Windows Server 2003 (70-290) М.: ЭКОМ; БИНОМ. Лаборатория знаний, 2006. 447 с.
6. Згуровський М. Проблеми інформаційної безпеки в Україні, шляхи їх вирішення // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Київ. 2018. С. 10-14.
7. Кузнецов О. О. Захист інформації в інформаційних системах: навч. посіб. Х.: ХНЕУ, 2018. 510 с.
8. Рассел Ч., Кроуфорд Ш., Microsoft Windows Server 2003: Справочник администратора.; пер. с англ. Дж. Джеренд. М.: ЭКОМ, 2006. 1424 с.
9. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с. англ. М.: Издательский дом «Вильямс», 2011. 672 с.
10. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учеб. для вузов. 4-е изд. СПб.: Питер, 2011. 944 с.
11. Поляков А. О., Євсєєв С. П., Огурцов В. В. Лабораторний практикум з навчальної дисципліни «Захист інформації в інформаційних системах»: навч.-практ. посіб. Х.: ХНЕУ, 2017. 208 с.
12. Поповский В. В., Персиков А. В. Защита информации в телекоммуникационных системах: Учебник в 2-х т. Харьков: ООО «Компания СМИТ», 2006. 238 с.
13. Рибальський О. В., Смаглюк В. М., Хахановський В. Г. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України. К.: НАВС, 2013. 255 с.
14. Рибальський О. В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації. Навчальний посібник для курсантів ВНЗ МВС України. К.: Вид. Національної академії внутріш. справ, 2013. 104 с.
15. Yullia Franko, Natalia Porplytsya, Mykhailo Ozhha, Olha Potapchuk, Yuriy Franko / Method and Software for Solving the Problem of Fuzzy Matching of Records in Relative Databases // 2021 11th International Conference on Advanced Computer Information Technologies, ACIT 2021 – Proceedingsthis link is disabled, 2021, pp. 696-699.
16. Mikhail Divizinyuk, Iryna Lutsyk, Volodymyr Rak, Natalia Kasatkina, Yuriy Franko / Mathematical Model of Identification of Radar Targets for Security of Objects of Critical Infrastructure // 2021 11th International Conference on Advanced Computer Information Technologies, ACIT 2021 – Proceedingsthis link is disabled, 2021, pp. 696-699.

17. Hevko Ihor Vasilievich, Franko Yuri Pavlovich. Use of modern information and communication technologies in the process of preparation of future bachelors of motor transport. Journal of Education, Health and Sport. 2020;10(4): pp. 280-288.
18. Douglas E. Internetworking with TCP/IP, Vol. III: Client-Server Programming and Applications, Linux / E. Douglas, D. Comer, L. Stevens. Posix Sockets Version. Addison-Wesley, 2010. 601 p.

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 таким 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 силабусу 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.