ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФІЗИЧНИЙ ФАКУЛЬТЕТ
Кафедра твердотільної електроніки та інформаційної безпеки

«ЗАТВЕРДЖУЮ»
Декан фізичного факультету
_____ /Лазур В.Ю./
«30» серпня 2023 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕХНОЛОГІЇ АДМІНІСТРУВАННЯ ТА ЕКСПЛУАТАЦІЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Рівеньвищої освіти	Другий (магістерський) рівень
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Освітня програма	Безпека інформаційних і комунікаційних систем
Статус дисципліни	Обов’язова
Мова навчання	Українська

Ужгород 2023

Робоча програма навчальної дисципліни «Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем» для здобувачів вищої освіти галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека та захист інформації освітньої програми Безпека інформаційних і комунікаційних систем.

Розробник: Пригара М.П., кан. техн. наук, доц. кафедри ТМ

Робочу програму розглянуто та затверджено на засіданні кафедри ТМ;

Пригара М.П. к.т.н., доцент кафедри ТМ.

Методичні рекомендації розглянуто та затверджено на засіданні кафедри
твердотільної електроніки та інформаційної безпеки

протокол № 9 від « 15 » червня 2023 р.

Завідувач кафедри _____ Різак В.М.

Схвалено науково-методичною комісією фізичного факультету

протокол № 10 від « 28 » червня 2023 р.

Голова науково-методичної комісії _____ Карбованець М. І.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td colspan="2">Розподіл годин за навчальним планом</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількістькредитів ЄКТС – 4</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальнакількість годин – 120</td><td>120</td><td></td></tr>
<tr><td>Кількістьмодулів – 2</td><td colspan="2">Семестр:</td></tr>
<tr><td></td><td>1-й,</td><td></td></tr>
<tr><td rowspan="5">Тижневих годин – для денної форми навчання: аудиторних –3 самостійної роботи студента – 4</td><td colspan="2">Лекції:</td></tr>
<tr><td>24</td><td></td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="5">Вид підсумкового контролю: залік, екзамен</td><td colspan="2">Лабораторні:</td></tr>
<tr><td>24</td><td></td></tr>
<tr><td colspan="2">Індивідуальна робота:</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="2">Форма підсумкового контролю: усна</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>72</td><td></td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Мета навчальної дисципліни є навчити студентів сучасним методам адміністрування захищених програмно апаратних комплексів та комп’ютерних мереж.

Відповідно до освітньої програми, вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

Інтегральна компетентність

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

Загальні компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-5. Здатність діяти соціально відповідально та громадсько свідомо.

КЗ-6. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).

Загальні компетентності (ЗК) згідно професійного стандарту «Фахівець сфери захисту інформації»

ЗК.01. Здатність діяти соціально відповідально та громадсько свідомо.

ЗК.02. Здатність застосовувати знання у практичних ситуаціях, розв’язувати завдання/задачі та практичні проблеми у професійній діяльності.

ЗК.03. Здатність оцінювати та забезпечувати якість виконуваних робіт.

ЗК.04. Здатність до абстрактного мислення, аналізу та синтезу, вчитися і бути сучасно навченим.

ЗК.05. Здатність до адаптації та дії в новій ситуації.

Фахові компетентності

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної

інфраструктури.

КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Професійні компетентності (за трудовою дією або групою трудових дій) згідно професійного стандарту «Фахівець сфери захисту інформації»

Д2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування щодо систем технічного та криптографічного захисту інформації.

Е2. Здатність взаємодіяти із керівництвом і фахівцями технологічних та інших підрозділів підприємства/організації з технологічних та інших питань, пов'язаних із забезпеченням захисту інформації та кіберзахисту.

Е3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень.

Е4. Здатність надавати консультативні послуги та технічну допомогу з питань технічного та криптографічного захисту інформації та кіберзахисту.

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Передумов вивчення навчальної дисципліни " Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем " немає.

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Безпека інформаційних і комунікаційних систем»,** вивчення навчальної дисципліни **«Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем»** повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також

аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

РН24. Володіти методиками аналізу, синтезу, оптимізації та прогнозування якості процесів функціонування інформаційних процесів та технологій в розподілених інформаційно- комунікаційних системах.

5. Методи контролю

Види контролю:

Поточне тестування студентів здійснюється через:

- бланкове тестування;
- оцінювання практичних навичок;
- оцінювання виконання самостійної роботи студентів.

Серед методів контролю: оцінювання практичних робіт та сформованих навичок, оцінювання доповідей, виконання різнорівневих завдань, бланкове тестування тощо.

Підсумкова оцінка отримується студентом за результатами всіх видів поточного контролю та результату іспиту.

Розподіл балів, які отримують студенти
Критерії та шкала оцінювання: національна та ECTS

Реалізація основних завдань контролю знань здобувачів вищої освіти в ОНУ досягається системними підходами до оцінювання та комплексністю застосування різних видів контролю. Згідно з діючою в університеті системою комплексної діагностики знань здобувачів вищої освіти, з метою стимулювання планомірної та систематичної навчальної роботи, оцінка знань здійснюється за 100-баловою системою, яка переводиться відповідно у національну шкалу («відмінно», «добре», «задовільно», «незадовільно») та шкалу європейської кредитно-трансферної системи (ЄКТС –A, B, C, D, E, FX, F).

Підсумковий семестровий контроль проводиться у формі іспиту в обсязі навчального матеріалу, що визначений навчальною програмою, та в терміни, встановлені графіком навчального процесу. При семестровому контролі отримані здобувачем згідно кредитно-трансферної системи оцінювання знань переводяться в оцінки за національною шкалою та за шкалою ЄКТС.

Комплексний показник успішності здобувача другого рівня вищої освіти, його обізнаності в предметі, що вивчається, характеризує якість його знань, систематичність, творчість, активність та самостійність. Максимальна сума балів за всі види робіт (контрольні, самостійне вивчення, практичні (семінарські) заняття) з даного курсу становить 100 балів.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота								**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	20	**60**
5	5	5	5	5	5	5	5		

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне оцінювання та самостійна робота							**Модульна контрольна робота**	**Сума**
Т9	Т10	Т11	Т12	Т13	Т14	Т15	20	**60**
6	6	6	5	6	5	6		

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	**Модуль 1**		**Модуль 2**	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Практичні заняття	6	40	6	40
Разом		**40**		**40**

Критерії оцінювання модульної контрольної роботи

Завдання для **модульної контрольної роботи** складається з 4 питань, кожне з яких оцінюється максимально у 5 балів. При оцінюванні кожного завдання контрольної роботив раховується обсяг і правильність виконаних завдань: оцінка "відмінно" ставиться за правильне виконання всіх завдань; оцінка "добре" ставиться за виконання 75 % усіх завдань; оцінка "задовільно" ставиться, якщо правильно виконано більше 50% запропонованих завдань; оцінка "незадовільно" ставиться, якщо завдань виконано менше від 50 %.. Неявка на модульну контрольну роботу – 0 балів.

Критерії оцінювання підсумкового семестрового контролю

Усі завдання, передбачені програмою, мають бути виконані у встановлені терміни. Якщо студент/ка був/ла відсутній на заняттях, він/вона мають можливість відпрацювати навчальні питання та завдання під час самостійної підготовки та обов'язково звітують про опанування навчального матеріалу викладачу. Студенти, які пропустили більше 30% з тих занять, де було передбачено оцінювання, не відзвітували за індивідуальну та самостійну роботу, до семестрового контролю не допускаються. У разі коли студент/ка не виконав/ла умови допуску до складання семестрового контролю, завчасно, але не пізніше трьох робочих днів до складання семестрового контролю, рішенням кафедри йому/їй встановлюється індивідуальний термін ліквідації заборгованості. Якщо заборгованість неліквідована у визначений кафедрою термін, то студент/ка вважається таким/ою, що не виконав/ла вимоги робочої програми навчальної дисципліни і у відомості обліку успішності йому/їй виставляється оцінка «незараховано» за національною шкалою і FX – за шкалою ЄКТС. При повній відсутності позитивних поточних оцінок, за визначені звітності, і не ліквідації заборгованості у визначений кафедрою термін, студенту курс з навчальної дисципліни не зараховується і в графі "підсумкова оцінка", йому виставляється оцінка "недопущений" за національною шкалою і F за шкалою ЄКТС. У такому випадку студенту/ці йому пропонується пройти повний курс повторно. У разі відмови його/її відраховують з університету.

Іспит отримує студент/ка, що виявив/ла знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, ознайомлений/на з рекомендованою літературою. Підсумкова оцінка розраховується за накопичувальною системою. При цьому максимальна кількість балів встановлюється наступним чином: за змістовий модуль №1 – 100 балів; за змістовий модуль №2 – 100 балів.

При виставленні оцінки враховуються результати навчальної роботи здобувача протягом семестру.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	ОцінкаECTS	Оцінка за національною шкалою	
		Екзамен та диференційований залік	Залік
90 – 100	**A**	відмінно	Зараховано
82-89	**B**	добре	
74-81	**C**		
64-73	**D**	задовільно	
60-63	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	Не зараховано
0-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	

За бажанням студента результуюча підсумкова екзаменаційна оцінка може бути визначена як інтегрована оцінка засвоєння всіх тем дисципліни і кількісно дорівнює середньому арифметичному балів, отриманих за кожний модуль.

Результати підсумкового контролю знань заносяться до екзаменаційної відомості.

Дотримання академічної доброчесності

Під час навчання учасники освітнього процесу зобов'язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил (https://vumonline.ua/course/academic-integrity-at-the-university/), якими мають керуватися учасники освітнього процесу з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності науково-педагогічним складом передбачає: посилання на джерела інформації у разі використання ідей, тверджень, відомостей; надання достовірної інформації про результати досліджень та власну педагогічну (науково-педагогічну, творчу) діяльність.

Дотримання академічної доброчесності здобувачами освіти передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання; посилання на джерела інформації у разі використання ідей, тверджень, відомостей; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності як: повторне проходження оцінювання (підсумковий модульний контроль, підготовка індивідуального завдання за іншою темою тощо).

Перевірка індивідуальних робіт здобувачів на наявність академічного плагіату проводиться викладачем або спеціально призначеним для цього працівником УжНУ за допомогою програмного продукту, що використовується в УжНУ з визначення рівня унікальності роботи.

6. Зміст навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1. «Адміністрування Windows»

***Тема 1*. Адміністрування Windows.**

Встановлення. Початкове налаштування. Сервери Windows. Основні мережеві налаштування.

Література: 1, 4, 5.

Тема 2. **Віртуалізація.**

Поняття віртуалізації. Контейнеризація. Докер. Види віртуальних машин.Література: 1, 2, 6.

Тема3. **Встановлення і початкове налаштування Windows Server.**

Базове мережеве налаштування. Розгортання системи через мережу. Встановлення Active Directory

Література: 2, 3, 5.

Тема 4. **Основні концепції Active Directory.**

Основні концепції служби каталогів. Профілі користувачів. Квотування диску. Розмежування прав.

Література: 1, 2, 4, 5.

Тема 5. **Файлові системи.**

Файлова система FAT16, Файлова система FAT32, Файлова система NTFS. Файлові системи хмарного зберігання даних.

Література: 2, 4, 5.

Тема 6. **Використання групових політик.**

Створення власних групових політик, базові налаштування. Локальні та глобальні групові політики. Розподіл прав.

Література: 1, 2, 5.

Тема 7. **Сервери DHCP і DNS.**

Базові налаштування сервера DHCP. Налаштування DNS сервера на контролерідомену.

Література: 1, 2, 3, 7.

Тема 8. **Встановлення і налаштування Domain Controller.**

Поняття домену. Сервери в середині домену. Групові політики контроллера домену, Профілі користувачів та авторизація.

Література: 1, 2, 5, 8.

ЗМІСТОВИЙ МОДУЛЬ 2. «Адміністрування Linux»

Тема 9. **Планування і розгортання Linux.**

Ієрархія версій. Встановлення Linux. Розподіл дискового простору. Вибір пакетів. Графічні оболонки.

Література: 1, 4, 5, 9.

Тема 10. **Файлові системи, диски і розділи.**

Робота з файловими системами EXT3, EXT4. Призначення розділу SWAP. Робота з файловими системами. Файл fstab. Монтування пристроїв.

Література: 1, 2, 5, 6.

Тема 11. **Програмний комплекс для віддаленого керування системою Webmin.**

Встновлення Webmin. Базові налаштування Apache server. Віддалений доступ через telnet та SSH

Література: 1, 4, 5, 9.

Тема 12. **Міжмережевий екран IPTABLES.**

Поняття файерволу. Трансляція адрес. Міжмережева взаємодія. Пакет Iptables. Пакет IPChains.

Література: 2, 4, 5.

Тема 13. **Проксі-сервер SQUID.**

Поняття проксі сервера. Налаштування сервера SQUID. Прозорий проксі сервер. Можливості авторизації через проксі сервер.

Література: 4, 10.

Тема 14. **Файловий сервер SAMBA.**

Протокол SMB. Спільний доступ до файлів принтерів та папок. Базові налаштування сервера SAMBA**.**

Література: 6, 7, 10.

Тема 15. **Засоби створення резервних копій. RAID-масиви.**

Поняття резервного копіювання. RAID-масиви. Автоматичні резервні копії.

Відновлення з резервної копії.Література: 6, 7, 9,10.

7. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин					
	Форма навчання: денна					
	Усього	у тому числі				
		лекції	практичні (семінарські)	лабораторні	індивідуальна робота	самостійна робота
1-й семестр						
Змістовий модуль 1						
Тема 1. Адміністрування Windows	7	1				4
Тема 2. Віртуалізація	7	1				4
Тема 3. Встановлення і початкове налаштування Windows Server.	8	2		2		4
Тема 4. Основні концепції Active Directory.	8	2		2		4
Тема 5. Файлові системи	8	2		2		4
Тема 6. Використання групових політик.	7	1		2		4
Тема 7. Сервери DHCP і DNS.	7	1		2		4
Тема 8 Встановлення і налаштування Domain Controller	8	2		2		4
Модульна контрольна робота						
Разом за модуль	56	12		12		32
Змістовий модуль 2						
Тема 9. Файлові системи, диски і розділи.	18	2		2		4
Тема 10. Планування і розгортання Linux	24	2		2		8
Тема 11. Програмний комплекс для віддаленого керування системою Webmin.	12	2		2		6
Тема 12. Міжмережевий екран IPTABLES.	10	1				6
Тема 13. Проксі-сервер SQUID.		2		2		6
Тема 14. Файловий сервер SAMBA.		1		2		6
Тема 15. Засоби створення резервних копій. RAID-масиви.		2		2		6
Модульна контрольна робота						
Разом за модуль	64	12		12		40
Разом за семестр	**120**	**24**		**24**		**72**

8. ТЕМИ СЕМІНАРСЬКИХ ТА ЛАБОРАТОРНИХ ЗАНЯТЬ

№ з/п	Тема	Кількість годин
1	Встановлення і початкове налаштування Windows Server.	4
2	Налаштування Active Directory	2
3	Використання групових політик	2
4	Встановлення і налаштування Domain Controller	2
5	Планування і розгортання Linux.	4
6	Програмний комплекс для віддаленого керування системою Webmin.	2
7	Отримати практичні навики з налаштування IPTABLES	2
8	Отримати практичні навики з налаштування SQUID	4
9	Отримати практичні навики з налаштування SAMBA.	2
Разом		24

9. ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

Начальним планом не передбачені

10. ОРГАНІЗАЦІЯ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

Завдання для самостійної роботи студентів

Самостійна робота студентів під час вивчення даного навчального курсу включає теоретичну підготовку з окремих тем курсу, що вивчаються в порядку самостійної роботи, а також підготовку до практичних занять з тем, що вказані вище.

Місце виконання самостійної роботи

Самостійна робота студента над засвоєнням навчального матеріалу виконується у бібліотеці, навчальних аудиторіях і лабораторіях, комп'ютерних класах, а також у домашніх умовах.

№п/п	Тематика	К-сть годин
1	Сертифікації та вміння системного адміністратора.	4
2	Посадові обов’язки і спеціалізація системного адміністратора.	4
3	Плюси і мінуси професії “системний адміністратор”. Перспективи. Попит.	4
4	Основні поняття віртуалізації.	4
5	Віртуальна машина.	4
6	Технології віртуалізації.	4
7	Планування і встановлення системи Windows Server.	6
8	Файлові системи, диски і розділи Windows Server.	4
9	Сервери DHCP і DNS Windows Server.	6
10	Основні концепції Acfve Directory.	4
11	Використання групових політик Windows Server.	6
12	Налаштування параметрів безпеки сервера.	6
13	Додаткові сервіси Windows Server.	4
14	Планування і розгортання Linux.	6
15	Файлові системи, диски і розділи Linux.	6
Разом:		**72**

До самостійної роботи відноситься: підготовка до лекцій, практичних, семінарських, лабораторних занять; написання рефератів, ессе; опрацювання відеоматеріалів, робота в мережі Інтернет, складання тестів, кросвордів, ситуаційних завдань.

11. ІНДИВІДУАЛЬНЕ НАВЧАЛЬНО-ДОСЛІДНЕ ЗАВДАННЯ

Не заплановане.

12. Методи навчання

Заняття із дисципліни проводяться у формі: лекцій з використанням наочних матеріалів, посібників, мультимедійних технологій; практичних занять; самостійної роботи з основною та додатковою літературою, періодичними виданнями, джерелами в інтернеті.

Серед методів навчання використовуються: *словесні* (пояснення, розповідь, інструктажі, ситуативне моделювання, ситуативне навчання, оксфордскі дебати, мозковий штурм, аналіз відео- і фотоматеріалів, обмін думками, захист доповідей тощо); *наочні* (демонстрування, мультимедійні презентації); *практичні* (ділові (рольові) ігри, розв’язання ситуаційних задач, аналіз статистичних даних, метод проєктів, відпрацювання практичних навичок тощо) методи.

13. Методичне та матеріально-технічне забезпечення

Методичне забезпечення: робоча програма навчальної дисципліни; навчальна програма дисципліни; мультимедійний супровід матеріалів лекцій та семінарських занять; план семінарських занять. Різноманітні прилади, необхідні для ведення практичних занять; засоби індивідуального захисту.

1.Тексти лекцій.

2.Ілюстративний матеріал: слайди, таблиці, презентації.

14. Рекомендована навчальна та навчально-методична література

1. Бикманс Герард. Linux from Scratch. Version 8.4, 2019. — 368 с.
2. Васильєва Н.К. та ін. Інформатика в LINUX-середовищі, Навч. посібник / кол. авт.; за ред. Н.К. Васильєвої. — Дніпропетровськ: Біла К., 2016. — 267 с.
3. Основи адміністрування LAN у середовищі MS Windows. Навчальний посібник / Б. А. Демида, К. М. Обельовська, В. С. Яковина. Львів: Видавництво Львівської політехніки, 2013. 488 с
4. Wiki DHCP. - [Електронний ресурс]. - Режим доступу: http://en.wikipedia.org/wiki/DHCP.
5. Microsoft DHCP. - [Електронний ресурс]. - Режим доступу: http://technet.microsoft.com/en-us/network/bb643151 .aspx
6. Microsoft Corporation Microsoft Windows 7. Group Policy for Beginners. Published: April 2011. - [Електронний ресурс]. - Режим доступу: http://technet.microsoft.com/ru-ru/library/
7. Захист операційного середовища систем Інтернет голосування/ВМ Чуприн, ВМ Вишняков, МП Пригара -// Захист інформації, 2017 - Режим доступу: https://jrnl.nau.edu.ua/index.php/ZI/article/download/11444/15347
8. Захищена система технічної підтримки процесів дистанційного волевиявлення- Режим доступу: https://dspace.nau.edu.ua/bitstream/NAU/34672/5/diss_Prygara.pdf
9. To install the default LAMP stack in Ubuntu 10.04 and above - Режим доступу: https://help.ubuntu.com/community/ApacheMySQLPHP
10. Lee, James; Brent Ware (December 2002). Open Source Web Development with LAMP: Using Linux, Apache, MySQL, Perl, and PHP. Addison Wesley. ISBN 0-201-77061-X. - Режим доступу: https://archive.org/details/opensourcewebdev0000leej
11. Налаштування детального запису операцій із файлами на Samba-сервері - Режим доступу: http://avz.org.ua/wp/2010/03/05/samba-detailed-logging/
12. Setting up Samba as an Active Directory Domain Controller- Режим доступу: https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller