**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**Волинський національний університет імені Лесі Українки**
**Факультет інформаційних технологій і математики**
**Кафедра комп'ютерних наук та кібербезпеки**

# СИЛАБУС
**нормативного освітнього компонента**

# БЕЗПЕКА ІНФРАСТРУКТУРИ КОМП`ЮТЕРНИХ МЕРЕЖ

**підготовки** бакалавра

**спеціальності** 125 Кібербезпека

**освітньо-професійної програми** Інформаційна безпека

Луцьк – 2022

**Силабус навчальної дисципліни «**Безпека інфраструктури комп`ютерних мереж**»** підготовки бакалаврів галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека за освітньою програмою Інформаційна безпека

**Розробник:** доцент, кандидат технічних наук Багнюк Наталія Володимирівна

**Погоджено**
Гарант освітньо-професійної програми:

Глинчук Л.Я.

**Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки**

протокол № 3 від 13 жовтня 2022 р.

Завідувач кафедри:

Гришанович Т. О.

## І. Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика освітнього компонента</th></tr>
<tr><td>Денна форма навчання</td><td rowspan="4">12 Інформаційні технології<br><br>125 Кібербезпека<br><br>Інформаційна безпека</td><td>Нормативна</td></tr>
<tr><td rowspan="2">Кількість годин / кредитів<br>120 / 4</td><td>Рік навчання 3<br>Семестр 6</td></tr>
<tr><td>Лекції 34 год.</td></tr>
<tr><td rowspan="2">ІНДЗ: немає</td><td>Лабораторні 34 год.</td></tr>
<tr><td rowspan="2">Перший (бакалаврський)</td><td>Самостійна робота 44 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td>Мова навчання</td><td>Форма контролю: екзамен</td><td>українська</td></tr>
</table>

## ІІ. Інформація про викладачів

| | |
|---|---|
| ПІП | Багнюк Наталія Володимирівна |
| Науковий ступінь | кандидат технічних наук |
| Вчене звання | доцент |
| Посада | доцент кафедри комп’ютерних наук та кібербезпеки |
| Контактна інформація | (095) 55 25 009, bahniuk.nataliia@vnu.edu.ua |
| Дні занять | за розкладом http://94.130.69.82/cgi-bin/timetable.cgi?n=700 |

## ІІІ. Опис освітнього компонента

### 1. Анотація курсу

Дисципліна «Безпека інфраструктури комп`ютерних мереж» належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра, присвячена вивченню: загроз безпеці, з якими стикається сучасна мережева інфраструктура; захисту мережевої інфраструктури; реалізації AAA на маршрутизаторах, використовуючи локальну базу даних маршрутизаторів і зовнішні сервери AAA; пом’якшенню загрози для маршрутизаторів і мереж за допомогою списків контролю доступу (ACL); впровадження безпечного проектування мережі, керування і звітування; реалізації набору функцій брандмауера, пом’якшення поширених атак рівня 2, впровадження VPN.

З метою кращого засвоєння навчального матеріалу дисципліни студенти повинні до його початку опанувати знаннями з таких предметів: сучасне програмне забезпечення та хмарні технології, системи моніторингу загроз, організаційне забезпечення захисту інформації, діагностика шкідливого програмного забезпечення, комп'ютерні мережі.

Найбільш яскраво виражені міждисциплінарні зв’язки з діагностикою шкідливого програмного забезпечення, комп'ютерними мережами, захистом інформації в операційних системах, захистом інформації в інформаційно-комунікаційних системах.

### 2. Мета і завдання освітнього компонента

**Метою** викладання дисципліни "Безпека інфраструктури комп'ютерних мереж" є підготовка фахівців, що володіють сучасним підходом до організації безпечної мережевої інфраструктури, вміють детектувати загрози в мережі та протидіяти їм.

**Завдання**: теоретична та практична підготовка студентів з питань сучасних принципів та методів організації процесів безпеки в сучасній мережевій інфраструктурі

## 3. Результати навчання та компетентності

Вивчення навчальної дисципліни «Безпека інфраструктури комп`ютерних мереж» сприяє формуванню та розвитку у здобувачів таких загальних та спеціальних компетентностей:

- вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. (**ЗК 4**);
- здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки (**ФК 2**);

Очікувані програмні результати навчання, які забезпечуються зокрема освітнім компонентом «Безпека інфраструктури комп`ютерних мереж» у комплексі з іншими компонентами освітньої програми:

- діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки (**ПРН 7**);
- вирішувати задачі аналізу програмного коду на наявність можливих загроз. **(ПРН 53).**

## 4. Структура освітнього компонента

| **Назви змістових модулів і тем** | **Кількість годин** | | | | | **Форма контролю / Бали** |
|---|---|---|---|---|---|---|
| | **Усього** | **у тому числі** | | | | |
| | | **Лекції** | **Лабораторні заняття** | **Консультації** | **Самостійна робота** | |
| Змістовий модуль 1. | | | | | | |
| Тема 1. Основи захисту мереж | 4 | 1 | | 1 | 2 | Зах. ЛР |
| Тема 2. Мережеві загрози | 4 | 1 | | 1 | 2 | Зах. ЛР |
| Тема 3. Пом'якшення загроз | 4 | 1 | | 1 | 2 | Зах. ЛР |
| Тема 4. Безпечний доступ до пристрою | 6 | 1 | 2 | 1 | 2 | Зах. ЛР |
| Тема 5. Призначення адміністративних ролей | 6 | 2 | 2 | | 2 | Зах. ЛР |
| Тема 6. Моніторинг та управління пристроями | 6 | 2 | 2 | | 2 | Зах. ЛР |
| Тема 7. AAA | 6 | 2 | 2 | | 2 | Зах. ЛР |
| Тема 8. Списки контролю доступу | 6 | 2 | 2 | | 2 | Зах. ЛР |
| Тема 9. Технології брандмауера | 6 | 2 | 2 | | 2 | Зах. ЛР |
| Тема 10. Політики на основі зони | 5 | 1 | 2 | | 2 | Зах. ЛР |
| Тема 11. Технології IPS | 5 | 1 | 2 | | 2 | 20 б. |
| **Разом за змістовим модулем 1** | **58** | **16** | **16** | **4** | **22** | **20 б.** |
| Змістовий модуль 2. Основи комутації, маршрутизації та бездротового зв’язку | | | | | | |
| Тема 12. Експлуатація та впровадження IPS | 5 | 1 | 1 | 1 | 2 | Зах. ЛР |
| Тема 13. Безпека кінцевих точок | 5 | 1 | 1 | 1 | 2 | Зах. ЛР |
| Тема 14. Безпека другого рівня | 5 | 1 | 1 | 1 | 2 | Зах. ЛР |
| Тема 15. Криптографічні послуги | 5 | 1 | 1 | 1 | 2 | Зах. ЛР |
| Тема 16. Цілісність та достовірність | 6 | 2 | 2 | | 2 | Зах. ЛР |

| | | | | | | |
|---|---|---|---|---|---|---|
| Тема 17. Криптографія з відкритими ключами | 6 | 2 | 2 | | 2 | Зах. ЛР |
| Тема 18. VPN | 6 | 2 | 2 | | 2 | Зах. ЛР |
| Тема 19. Впровадження VPN-мережі IPsec між сайтами | 6 | 2 | 2 | | 2 | Зах. ЛР |
| Тема 20. Вступ до ASA | 6 | 2 | 2 | | 2 | Зах. ЛР |
| Тема 21. Конфігурація брандмауера ASA | 6 | 2 | 2 | | 2 | Зах. ЛР |
| Тема 22. Тестування безпеки мережі | 6 | 2 | 2 | | 2 | Зах. ЛР |
| **Разом за змістовим модулем 2** | **62** | **18** | **18** | **4** | **22** | **20 б.** |
| **Всього годин / Балів** | **120** | **34** | **34** | **8** | **44** | **40 б.** |

| **Види підсумкових робіт** | **Бали** |
|---|---|
| Модульна контрольна робота за ЗМ 1 | 30 |
| Модульна контрольна робота за ЗМ 2 | 30 |
| **Всього балів за МКР** | **60** |

## 5. Завдання для самостійного опрацювання

Під час самостійної роботи здобувач освіти опрацьовує додатковий теоретичний матеріал згідно рекомендованих літературних джерел та виконує індивідуальні завдання. Питання, опрацьовані здобувачем на самостійній роботі, враховані в модульних контрольних роботах та при складанні іспиту.

| № п/п | Тема | К-сть годин |
|---|---|---|
| 1. | Принципи організації безпеки мережевої інфраструктури | 2 |
| 2. | Інформаційні технології та проблеми забезпечення їх безпеки | 2 |
| 3. | Принципи організації інформаційної безпеки | 2 |
| 4. | Моделі управління мережевими ресурсами | 2 |
| 5. | Програмно-апаратні засоби забезпечення безпеки мережі | 4 |
| 6. | Технічні (апаратні) засоби забезпечення захисту інформації | 2 |
| 7. | Технології забезпечення безпеки мережевої інфраструктури | 2 |
| 8. | Безпека міжмережевої взаємодії | 2 |
| 9. | Протокол міжмережного захисту Kerberos | 2 |
| 10. | Реалізація загроз інформації у мережах на основі протоколів TCP/IP | 8 |
| 11. | Впровадження VPN-мережі IPsec між сайтами | 8 |
| 12. | Вступ до ASA | 4 |
| 13. | Тестування безпеки мережі | 4 |
| **Разом:** | | **44** |

## IV. Політика оцінювання

Політика оцінювання та організація контрольних заходів здійснюється згідно з Положенням про поточне та підсумкове оцінювання знань здобувачів освіти Волинського національного університету імені Лесі Українки https://bit.ly/3RXsLvA .

Оцінювання навчальних досягнень з освітнього компонента здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах, вчасне і якісне виконання домашніх завдань, самостійне опрацювання теоретичного матеріалу) та підсумковий модульний контроль (письмові модульні контрольні роботи). Максимальна кількість балів, яку може накопичити здобувач під час поточного оцінювання за семестр – 40 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за модульні контрольні роботи (МКР). Максимальна кількість балів, яку може накопичити здобувач під час модульного контролю за семестр, складає 60 балів. Модульні контрольні роботи складаються з тестів по темах. Упродовж

семестру, після завершення відповідних тем (модулів), проводяться М1, М2 модульні контрольні роботи у тестовій формі.

Якщо за результатами семестру накопичено не менше 75 балів і здобувач погоджується із цим результатом, то оцінка за семестр може виставлятися без складання іспиту. В іншому разі студент складає іспит; максимальна кількість балів, яку можна отримати на іспиті – 60 балів. Вони замінюють бали модульного семестрового контролю, поточний семестровий контроль при цьому зберігається.

**1. Політика викладача щодо здобувача**

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загально-прийнятих морально-етичних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття без поважних причин; користування мобільним телефоном або іншими мобільними пристроями під час заняття не з навчальною метою, зокрема розмови, переписка, ігри та інші розваги; списування. Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу. У випадку запровадження дистанційної форми навчання, що може бути пов'язано із карантином, надзвичайними ситуаціями, воєнним станом і т. ін., заняття проводитимуться в режимі відео конференції Zoom та / або з використанням платформи Moodle https://moodle-cs.vnu.edu.ua/. Матеріал пропущених занять здобувач опрацьовує самостійно, звітує про виконання викладачу в індивідуальному порядку. Пропущені заняття не звільняють студента від вчасного виконання модульних контрольних робіт разом із групою.

Перезарахування окремих змістових модулів, модульних контрольних заходів в межах освітнього компонента регламентується Положенням про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки https://bit.ly/3Bdq6qP .

**2. Політика щодо академічної доброчесності**

Під час навчання учасники освітнього процесу зобов'язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності https://bit.ly/3BFUETR .

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання студенти не користуються забороненими засобами (мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси), самостійно виконують запропоновані завдання.

**3. Політика щодо дедлайнів та перескладання**

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона вивчають теоретичний матеріал самостійно використовуючи навчальні посібники, конспекти лекцій, виконують всі завдання для аудиторних занять, всі домашні завдання. Прозвітуватися про виконання завдань можна під час консультацій, одночасно при цьому з'ясувати незрозумілі моменти, задати запитання викладачу.

Перескладання модульних контрольних робіт заборонено. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.

## V. Підсумковий контроль

Якщо за результатами семестру накопичено не менше 75 балів і здобувач погоджується із цим результатом, то оцінка за семестр може виставлятися без складання іспиту. В іншому разі студент складає іспит; максимальна кількість балів, яку можна отримати на іспиті – 60 балів. Вони замінюють бали модульного семестрового контролю, поточний семестровий контроль при цьому зберігається. Екзамен проходить шляхом складання тесту. Оцінка за семестр у випадку складання іспиту є сумою балів поточного контролю та балів, отриманих під час іспиту.

### Перелік питань до іспиту

1. Принципи організації інформаційної безпеки
2. Захист від автоматичних засобів нападу
3. Організаційні принципи захисту даних
4. Принципи побудови системи забезпечення безпеки інформації в АС
5. Моделі управління мережевими ресурсами.
6. Поняття моделі управління робочою групою та доменна модель управління
7. Загрози інформації у мережах на основі протоколів TCP/IP
8. Поняття «віддалена атака»
9. Класифікація атаки на розподілені автоматизовані системи
10. Тенденції розвитку і застосування методів і засобів захисту інформації
11. в телекомунікаційних системах
12. Захист інформації в корпоративних мережах
13. Принципи та методи надання доступу до інформаційних ресурсів.
14. Профіль безпеки стандарту OSI/ISO 15408.
15. Системи виявлення вторгнень, їх типи
16. Методи і засоби аналізу безпеки програмного забезпечення
17. Контрольно-випробні методи аналізу безпеки програмного забезпечення
18. Логіко-аналітичні методи контролю безпеки програм.
19. Інформаційні технології та принципи організації інформаційної безпеки.
20. Види та властивості інформації як предмета захисту.
21. Інформаційні технології та проблеми їхньої безпеки.
22. Принципи організації інформаційної безпеки.
23. Моделі управління мережевими ресурсами.
24. Програмні та апаратні засоби захисту в інформаційних системах.
25. Технології захисту інформації при міжмережевій взаємодії.
26. Захист повідомлень при передачі каналами та лініями зв’язку.
27. Принципи побудови мережевих екранів.
28. Технології захисту у мережах на основі протоколів TCP/IP.
29. Реалізація загроз інформації у мережах на основі протоколів TCP/IP.
30. Принципи побудови мереж VPN.
31. Виявлення мережевих атак шляхом аналізу трафіка.
32. Основи захвату та аналізу мережевого трафіка.
33. Виявлення мережевих атак шляхом аналізу трафіка.
34. Надійність та стійкість програмного забезпечення.
35. Методи забезпечення стійкості та надійності програмного забезпечення
36. Загрози в архітектурі відкритих мереж в моделі OSI/ISO
37. Процедури та реалізація захисту в моделі OSI/ISO
38. Основні положення загальних критеріїв безпеки інформаційних технологій стандарту ISO 15408.
39. Функціональні вимоги до засобів захисту стандарту ISO 15408
40. Вимоги гарантій засобів захисту стандарту ISO 15408
41. Рівні гарантій безпеки стандарту ISO 15408
42. Потенційні загрози безпеці та типові завдання захисту стандарту ISO 15408

43. Профіль та проект захисту стандарту ISO 15408
44. Забезпечення безпеки на фізичному рівні моделі OSI.
45. Забезпечення безпеки на транспортному рівні моделі OSI.
46. Керування сеансами TCP. Протокол UDP.
47. Забезпечення безпеки на канальному рівні моделі OSI.
48. Забезпечення безпеки на рівні додатків моделі OSI.
49. Забезпечення безпеки на мережному рівні моделі OSI.
50. Планування захищеної мережі
51. Організація захищеного підключення
52. Особливості реалізації статичних і динамічних VLAN
53. Методика створення списків управління доступом (ACL)
54. Призначення і зміст списків управління доступом
55. Типи профілів доступу
56. Процес створення профілю доступу
57. Приклади налаштування ACL
58. Списки реалізації управління доступом (ACL)
59. Конфігурація брандмауера ASA
60. Технології IPS
61. Моніторинг та управління пристроями
62. Тестування безпеки мережі

## VI. Шкала оцінювання

| Оцінка в балах | Лінгвістична оцінка | Оцінка за шкалою ECTS | |
|---|---|---|---|
| | | оцінка | пояснення |
| 90–100 | Відмінно | A | відмінне виконання |
| 82–89 | Дуже добре | B | вище середнього рівня |
| 75–81 | Добре | C | загалом хороша робота |
| 67–74 | Задовільно | D | непогано |
| 60–66 | Достатньо | E | виконання відповідає мінімальним критеріям |
| 1–59 | Незадовільно | Fx | необхідне перескладання |

## VI. Рекомендована література та інтернет-ресурси

### Основна

1. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
2. Жаровський Р.О Конспект лекцій з дисципліни «Захист інформації у комп'ютерних системах» розроблені у відповідності з навчальним планом за спеціальністю 123 "Комп'ютерна інженерія". – Тернопіль, 2019. – 268 с.
4. Стислий словник основних термінів з безпеки інформаційних систем, технологій, кібербезпеки/ Харків. нац. ун-т ім. В. Н. Каразіна ; уклад. Віталій Іванович Єсін, Сергій Геннадійович Рассомахін. – Харків : ХНУ ім. В. Н. Каразіна, 2018. – 63 с. Режим доступу: http://surl.li/ezdsk
5. Коллинз М.. Защита сетей. Подход на основе анализа данных. М.:ДМК Пресс, 2020. 308 с.
6. Network Security Курс Мережевої академії Cisco Режим доступу: http://surl.li/ezdsj
13. Олещенко Л.М. Організація комп'ютерних мереж: лабораторний практикум [Електронний ресурс] : навч. посіб. для студ. / Л.М.Олещенко -Київ : КПІ ім. Ігоря Сікорського, 2018. - 137 с.
14. Ахрамович В.М., Чегренець В.М, Котенко А.М. Комп'ютерні мережі. Практикум / В.М. Ахрамович, В.М. Чегренець, А.М. Котенко // Державний університет телекомунікацій. – К.: ДУТ, 2018. – 412 с.

**Додаткова**

1. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К. : НАУ. – 2013. – 432 с.
2. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія / Д. В. Дубов. – К.: НІСД, 2014. – 328 с.
3. Tanenbaum A. et al. Computer Networks Title: Computer Networking: A Top-Down Approach //Instructor. – 2019. – Т. 201901 http://surl.li/audtv (дата звернення: 20.08.2022).
4. Оліфер, В. Г. Безпека комп'ютерних мереж / В. Г. Оліфер, Н. А. Оліфер. – М:, 2017. – 644 с.
5. Коллінз М.. Захист мереж. Подхід на основі аналізу даних. М.:ДМК Пресс, 2020. 308 с.
6. Оліфер В., Оліфер Н. Компьютерні мережі. Принципи, технології, протоколи. СПб.: Питер, 2020. 1008 с.
7. Комп'ютерні мережі : підручник / Блозва А. І., Матус Ю. В., Касаткін Д. Ю. Нац. ун-т біоресурсів і природокористування України. – Київ : Компринт, 2019 . – 382 с. http://surl.li/eoiuk (дата звернення: 20.08.2022).
8. Адресації в IP-мережах. Теоретичні основи та приклади розв'язання задач: навч. посібник / Д.І. Могилевич, І.В.Кононова. – Київ: КПІ ім. Ігоря Сікорського, 2019. – 55 с. http://surl.li/eoiul
9. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Проектування комп'ютерних систем та мереж : навч. посіб. — Кропивницький: Видавець Лисенко В. Ф., 2019. — 264 с. http://surl.li/eoiuo
10. Карпенко М. Ю. Конспект лекцій з курсу «Комп'ютерні мережі» (для студентів усіх форм навчання спеціальностей 122 – Комп'ютерні науки, 151 – Автоматизація та комп'ютерно-інтегровані технології, 126 – Інформаційні системи та технології) / М. Ю. Карпенко, Н. В. Макогон; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2019. – 99 с. URL: http://surl.li/cwnor (дата звернення: 15.07.2022)
11. Організація комп'ютерних мереж [Електронний ресурс]: підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Електронні текстові дані (1 файл: 45,7 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с. URL: http://surl.li/awegr (дата звернення: 22.07.2022).
12. Cisco Network Academy. Курс «Intro to Packet Tracer». [Електронний ресурс]. – Доступний з URL: https://www.netacad.com/courses/packet-tracer (дата звернення: 20.08.2022).
13. NetAcademy - Networking101Lite Перша сесія "Модель OSI/Мережі/Базові налаштування обладнання URL: http://surl.li/eoiux (дата звернення: 20.08.2022)
14. Networking101Lite Друга сесія "Другий (канальний) рівень OSI моделі. Ethernet. Комутація. VLAN URL: http://surl.li/eoiuy (дата звернення: 20.08.2022)
15. Networking101Lite Третя сесія "Третій (мережевий) рівень OSI моделі. IP. Маршрутизація URL: http://surl.li/eoiuz (дата звернення: 20.08.2022)
16. Networking101Lite Сесія №4 "Динамічне назначення IP адрес. DHCP URL: http://surl.li/eoivc (дата звернення: 20.08.2022)
17. Networking101Lite Сесія №5 "Мережева взаємодія. Сокети. Утиліти для мережевого інженера URL: http://surl.li/eoive (дата звернення: 20.08.2022)
18. Networking101Lite Сесія №6 " Контроль трафіку. Списки доступу. Налаштування контролю URL: http://surl.li/eoivg (дата звернення: 20.08.2022)
Networking101Lite Сесія №7 " Трансляція IP адрес. Доступ в Інтернет. NAT URL: http://surl.li/eoivi (дата звернення: 20.08.2022)
19. Networking101Lite Сесія №8 " VPN/Захист даних при передачі/IPSec URL: http://surl.li/eoivm (дата звернення: 20.08.2022)
20. Networking101Lite Сесія №9 "Динамічна маршрутизація/OSPF URL: http://surl.li/eoivq (дата звернення: 20.08.2022)
21. Networking101Lite Сесія №10 "Динамічна маршрутизація/bgp URL: http://surl.li/eoivr (дата звернення: 20.08.2022)

22. Computer networking: a top-down approach / James F. Kurose, University of Massachusetts, Amherst, URL: http://surl.li/eoivt (дата звернення: 20.08.2022)
23. Dr. Y Mohana Roopa Mr. P Ravinder Ms. N M Deepika URL: http://surl.li/eoivu (дата звернення: 20.08.2022)
24. Комп'ютерні мережі : навч. посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук ; Вінниц. нац. техн. ун-т. – Вінниця : ВНТУ, 2017. – 127 с.
http://surl.li/eoivv
25. Протокол IP. Статична маршрутизація в IP-мережах: навч. посібник / С.В. Панченко, С.І. Приходько, О.С. Жученко та ін. – Харків: УкрДУЗТ, 2017. – 136 с. http://surl.li/eoivz
26. Адміністрування комп'ютерних мереж та операційних систем: методичне видання / Укл. Поліщук В.В. – Ужгород: 2019. – 60 с. http://surl.li/eoiwe