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

«ЗАТВЕРДЖУЮ»
Декан фізичного факультету
_____/Лазур В.Ю./
«29» 04 2022 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИС ЦИПЛІНИ

ЗАХИСТ КОМУНІКАЦІЙНИХ МЕРЕЖ ЗАСОБАМИ CISCO

Рівень вищої освіти	**другий (магістерський) рівень**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
Предметна спеціальність (Спеціалізація) *(за наявності)*	
Освітня програма	**Системи технічного захисту інформації, автоматизація її обробки.**
Статус дисципліни	**вибіркова**
Мова навчання	**українська**

Ужгород 2022

Робоча програма навчальної дисципліни «**Захист комунікаційних мереж засобами Cisco**» для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека** освітньої програми **Системи технічного захисту інформації, автоматизація її обробки.**

Розробники: Маркевич П. В., ст. викладач кафедри ТЕІБ

Робочу програму розглянуто та затверджено на засіданні кафедри
твердотільної електроніки та інформаційної безпеки

протокол № 7 від «28» 04 2022р.

Завідувач кафедри _____ Різак В.М.

Схвалено науково-методичною комісією фізичного факультету

протокол № 10 від «29» 04 2022р.

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>Кількість кредитів ЄКТС - 4</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 120</td><td>1-й</td><td></td></tr>
<tr><td colspan="2">Семестр:</td></tr>
<tr><td rowspan="8">Тижневих годин
для денної форми навчання:

аудиторних – 3

самостійної роботи студента – 4</td><td>1-й</td><td></td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>18</td><td></td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Лабораторні:</td></tr>
<tr><td>24</td><td></td></tr>
<tr><td rowspan="2">Вид підсумкового контролю: залік</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>78</td><td></td></tr>
<tr><td>Форма підсумкового контролю: усна</td><td colspan="2"></td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою навчальної дисципліни «Захист комунікаційних мереж засобами Cisco» є формування у студентів розуміння принципів побудови комунікаційних мереж, що розгортаються на базі обладнання Cisco, а також забезпечення безпеки та надійності функціонування даних мереж.

Завданнями даного курсу є оволодіння теоретичних та практичних навичок побудови телекомунікаційних мереж з використанням обладнання Cisco, налаштування мережевого обладнання Cisco, вивчення архітектури та питань, пов'язаних із безпекою, експлуатацією та усуненням несправностей комунікаційних мереж.

Місце дисципліни в структурі освітньої програми: навчальна дисципліна **«Захист комунікаційних мереж засобами Cisco»** є вибірковим компонентом циклу професійної підготовки освітньої програми підготовки магістрів спеціальності «Системи технічного захисту інформації, автоматизація її обробки».

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

Інтегральна: здатність розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності:

1. Здатність застосовувати знання у практичних ситуаціях (КЗ-1).
2. Здатність проводити дослідження на відповідному рівні (КЗ-2).
3. Здатність до абстрактного мислення, аналізу та синтезу (КЗ-3).
4. Здатність оцінювати та забезпечувати якість виконуваних робіт (КЗ-4).
5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності) (КЗ-5).

Фахові компетентності:

1. 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 (КФ1).
2. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури (КФ3).
3. Здатність до дослідження, системного аналізу та забезпечення неперервності 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 (КФ5).
4. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації (КФ6).
5. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому (КФ7).
6. Здатність розробляти проектну документацію, програми та методики випробувань, налаштування та супровід комплексів захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури (КФ12).

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Системи технічного захисту інформації, автоматизація її обробки»**, вивчення навчальної дисципліни **«Захист комунікаційних мереж засобами Cisco»** повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

Програмні результати навчання	Шифр ПРН
Розробляти, застосовувати, інтегрувати, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі у сфері інформаційної безпеки та/або кібербезпеки.	ПРН4
Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	ПРН7
Досліджувати, розробляти і супроводжувати системи та засоби захисту інформації та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	ПРН8
Забезпечувати неперервність бізнес/операційних процесів, виявляти вразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	ПРН10
Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	ПРН11
Розробляти, супроводжувати й аналізувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	ПРН14
Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних й непередбачуваних ситуаціях, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень	ПРН16
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.	ПРН23

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни **«Захист комунікаційних мереж засобами Cisco»**:

Очікувані результати навчання з дисципліни	Шифр ПРН
Вміти інтегрувати, впроваджувати та удосконалювати сучасні інформаційні технології з метою забезпечення безпеки інформації в комунікаційних системах.	ПРН4
Вміти обґрунтовано використовувати, впроваджувати та аналізувати кращі світові практики та технічні рішення з метою вирішення завдань в галузі інформаційної безпеки та/або кібербезпеки комунікаційних систем.	ПРН7
Вміти проводити дослідження, здійснювати розробку і супровід систем та засобів захисту інформації та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	ПРН8
Забезпечувати неперервність бізнес/операційних процесів шляхом застосування навичок і вмінь з організації і побудови комунікаційних систем з	ПРН10

урахуванням ризиків для інформаційної безпеки та/або кібербезпеки організації..	
Бути спроможним до аналізу, контролю та забезпечення ефективного функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	ПРН11
Вміти розробляти, супроводжувати й аналізувати системи аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	ПРН14
Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних й непередбачуваних ситуаціях, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень	ПРН16
Здійснювати обґрунтований 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.	ПРН23

4. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни **«Захист комунікаційних мереж засобами Cisco»** є:

- залік;
- виконання завдань лабораторних робіт;
- стандартизовані тести;
- фронтальне та/або письмове опитування

Форми контролю та критерії оцінювання результатів навчання

Модульний контроль з навчальної дисципліни **«Захист комунікаційних мереж засобами Cisco»** складається з поточного контролю та модульного контрольного оцінювання результатів навчання.

Форми поточного контролю:

- фронтальне стандартизоване усне та/або письмове опитування за основними питаннями теми заняття;
- захист результатів лабораторної роботи;
- тестування;
- перевірка якості виконання завдань для самостійної роботи, зокрема за конспектами матеріалів.

Форма модульного контрольного оцінювання: письмова модульна контрольна робота та/або тестування.

Форма підсумкового семестрового контролю: залік.

До заліку допускаються студенти, які відпрацювали пропущені заняття і виконали модульні контрольні роботи та завдання для самостійної роботи. Контроль самостійної роботи здійснюється шляхом перевірки виконаних завдань на лабораторних та індивідуальних заняттях, під час захисту лабораторних робіт, тестування при поточному оцінюванні, презентації результатів виконаних завдань та досліджень.

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

Поточний контроль успішності						**Модульна контрольна робота**	**Сума**
Поточне оцінювання та самостійна робота							
Т1	Т2	Т3	Т4	Т5	Т6	60	**100**
5	5	10	5	5	10		

Т1, Т2 ... – теми

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

Поточний контроль успішності					**Модульна контрольна робота**	**Сума**
Поточне оцінювання та самостійна робота						
Т1	Т2	Т3	Т4	Т5	60	**100**
5	10	15	5	5		

Т1, Т2 ... – теми

Оцінювання окремих видів навчальної роботи з дисципліни «Захист комунікаційних мереж засобами Cisco»

Вид діяльності здобувача вищої освіти	**Модуль 1**		**Модуль 2**	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Лабораторні заняття (допуск, виконання та захист)	3	15	5	25
Комп’ютерне тестування при тематичному оцінюванні	2	25	1	15
Модульна контрольна робота	1	60	1	60
Разом		**100**		**100**

Критерії оцінювання модульної контрольної роботи

Модульна контрольна робота проводиться у письмовій формі шляхом відповідей на питання навчального модуля та вирішення тестових завдань. Кожна правильна відповідь

оцінюється певною кількістю балів. Максимальна кількість балів за кожний модуль становить 100 балів.

Критерії оцінювання підсумкового семестрового контролю

Підсумковий семестровий контроль з дисципліни **«Захист комунікаційних мереж засобами Cisco»** здійснюється у формі заліку, що проводиться в усній формі шляхом співбесіди. Результати заліку оцінюються за двобальною шкалою: „зараховано”, „незараховано”. Підсумкова оцінка визначається наступними критеріями:

Оцінка "зараховано" - якщо студент достатньо чітко і грамотно відповідає на питання в межах матеріалу, викладеного у рамках лекційних занять, може показати та обгрунтувати взаємозв'язок різних частин матеріалу, пройденого у межах матеріалу навчальної дисципліни; демонструє здатність до мислення, при відповіді на питання розмірковує, спираючись на отримані у рамках курсу знання, не допускає істотних неточностей у відповіді, правильно вибудовує логіку вирішення типових завдань;

Оцінка "незараховано" - якщо студент викладає основні питання недостатньо чітко або допускає істотні помилки при їх викладі, не може пояснити зв'язків у рамках викладеного матеріалу, не знає значної частини програмного матеріалу, не може дати точних визначень понять, пройдених у рамках курсу, дає розпливчасті формулювання і не володіє в належній мірі термінологією, плутається при відповіді на додаткові питання, не володіє прийомами вирішення типових завдань.

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

Переведення результатів, отриманих за 100-бальною шкалою оцінювання в національну 4-х бальну та шкалу за системою ECTS здійснюється за наступною схемою:

Оцінка за шкалою балів	Залік	ECTS	
		Оцінка	Характеристика
90-100	зараховано	A	відмінно
82-89		B	добре
74-81		C	добре
64-73		D	задовільно
60-64		E	задовільно
35-59	незараховано	FX	незадовільно з можливістю перескладання
1-34		F	незадовільно з обов'язковим повторним навчанням

Студент, який отримав за результатами підсумкового контролю оцінку «незараховано» або «незадовільно з обов'язковим повторним навчанням» (1-34 балів, F), зобов'язаний пройти повторний курс вивчення дисципліни (під час додаткового семестру) і скласти залік або екзамен.

Результати підсумкового контролю знань вносяться до відомості обліку успішності.

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1. Зміст навчальної дисципліни

Модуль 1. ОСНОВИ МЕРЕЖЕВОГО ЗЄДНАННЯ, ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ ПРОЦЕСІВ ТА БЕЗПЕКИ КАНАЛЬНОГО РІВНЯ МОДЕЛІ OSI.

Тема 1. Вступ. Основи мережевого з'єднання та передавання даних.

Сучасні мережеві технології та вплив мереж на наше життя. Компоненти мережі. Зображення мережі і топології. Основні типи мереж. Інтернет-з'єднання. Тенденції розвитку мереж та мережева безпека.
Базові налаштування кінцевих пристроїв та комутаторів. Доступ до Cisco IOS та навігація по операційній системі. Структура команд. Базові налаштування та збереження налаштувань. Порти і адреси. Налаштування IP-адресації.

Тема 2. Еталонні моделі OSI та TCP/IP.

Опис моделі OSI. Історія створення. Фізичний рівень, канальний рівень, мережевий рівень, транспортний рівень, рівень представлення та прикладний. Протоколи, що функціонують на відповідних рівнях моделі.
Опис моделі TCP/IP. Історія створення. Рівень доступу до мережі, міжмережевий рівень, транспортний рівень і прикладний. Протоколи, що функціонують на відповідних рівнях моделі.
Рух даних по рівнях моделей. Поняття PDU.
Порівняльна характеристика моделей.

Тема 3. Ethernet-концепції.

Фізичний рівень моделі OSI. Типи кабелів для здійснення комутацій обладнання. Мідний кабель, кабель вита пара. Волоконно-оптичний кабель. Бездротове зєднання.
Двійкова та шістнадцяткова системи числення.
WAN та LAN топології. Напівдуплексний та повнодуплексний зв'язок. Методи контролю доступу. Конкурентний доступ CSMA/CD. Конкурентний доступ з уникненням конфліктів CSMA/CA.
Кадри канального рівня. Структура кадру Ethernet. Адреси 2 рівня. Таблиця MAC-адрес.

Тема 4. Поняття комутації. Обладнання комутації, VLAN.

Методи пересилання кадрів на комутаторах Cisco. Наскрізна комутація. Буферизація пам'яті на комутаторах. Функція Auto-MDIX. Налаштування початкових параметрів комутатора. Команда boot system. Відновлення після системного збою. Версії ОС.
Налаштування портів комутатора. Захищений віддалений доступ. Перевірка зв'язку між безпосередньо під'єднаними мережами. Комутаційні домени. Домени колізій, широкомовні домени.
Огляд VLAN, магістральні та VLAN доступу.

Тема 5. Поняття маршрутизації. Обладнання маршрутизації, маршрутизація між VLAN.

Вступ до маршрутизації. Огляд базової конфігурації маршрутизатора. IPv4 та IPv6 пакети. Пересилання пакетів та визначення маршрутів. Статична та динамічна маршрутизація.
Принципи маршрутизації між VLAN. Маршрутизація між VLAN методом Router-on-a-Stick. Маршрутизація між VLAN за допомогою комутаторів 3 рівня. Виявлення і усунення несправностей маршрутизації між VLAN.

Тема 6. Безпека на 2 рівні моделі OSI та WLAN.

Принципи безпеки LAN. Безпека кінцевих точок, керування доступом. Загрози безпеці 2 рівня. Атаки на таблиці MAC-адрес. Переповнення таблиці MAC-адрес. Нейтралізація атак на таблиці MAC-адрес.
Атаки на локальну мережу. Атаки переходів між VLAN. Атаки з подвійними тегами VLAN. Атаки, направлені на DHCP, ARP-атаки та підроблення адрес. Атаки на STP.
Налаштування безпеки на комутаторі. Впровадження захисту портів. Стримування атак на VlAN та нейтралізація інших видів атак.

Модуль 2. МАРШРУТИЗАЦІЯ ТА БЕЗПЕКА НА 3 РІВНІ МОДЕЛІ OSI

Тема 1. Протоколи динамічної маршрутизації.

Еволюція протоколів динамічної маршрутизації. Принципи роботи протоколів динамічної маршрутизації. Поняття найкращого шляху. Балансування навантаження.
Протокол OSPF. Компоненти OSPF. Принцип роботи маршрутизації за станом каналу. OSPF для однієї та кількох зон. Типи пакетів OSPF. Оновлення стану каналу. Робочі стани OSPF, встановлення суміжності. Синхронізація баз даних OSPF.
Огляд, конфігурація та перевірка EIGRP. Сусідство і метрика EIGRP. Конвергенція EIGRP. Пасивні інтерфейси EIGRP. Налаштування статичного сусідства EIGRP, ідентифікатори маршрутизаторів.

Тема 2. Налаштування статичної маршрутизації.

Типи статичних маршрутів. Параметри наступного переходу. Команда статичного маршруту IPv4, IPv6. Початкові таблиці маршрутизації IPv4, IPv6.Статичний маршрут наступного переходу IPv4, IPv6. Безпосередньо під'єднаний статичний маршрут IPv4, IPv6. Повністю заданий статичний маршрут IPv4, IPv6. Перевірка статичного маршруту.
Змінні статичні маршрути. Налаштування змінних статичних маршрутів IPv4, IPv6. Перевірка змінних статичних маршрутів.
Налаштування статичних маршрутів вузла. Налаштування статичного маршруту вузла IPv6 з використанням локальної адреси каналу наступного переходу.

Тема 3. Безпека на 3 рівні моделі OSI.

Суб'єкти загроз та його засоби. Шкідливе програмне забезпечення та типові мережеві атаки. Загрози та вразливості IP. Вразливості UDP і TCP. Найкращі практики мережевої безпеки.
Списки контролю доступу. Призначення ACL і шаблонні маски. Рекомендації щодо створення ACL. Типи ACL для IPv4.
Налаштування стандартних ACL для IPv4. Захист VTY-ліній за допомогою стандартних ACL для IPv4. Налаштування розширених ACL для IPv4.

Тема 4. Резервування комунікаційних мереж.

Принципи роботи протоколу STP. Призначення протоколу, операції STP. Етапи створення топології без петель. Обрання кореневого мосту, визначення вартості кореневого шляху. Обрання кореневих, призначених та альтернативних портів.
Таймери STP. Єдальне дерево для кожної VLAN.
Розвиток STP. Версії та концепції. PortFast та BPDU Guard.
Принципи роботи та налаштування EtherChannel. Виявлення та усунення несправностей EtherChannel.

Тема 5. Оптимізація, контроль та усунення несправностей комунікаційних мереж.

Механізми QoS. Якість передавання даних у мережі. Характеристики мережевого трафіку. Алгоритми організації черг. Моделі якості обслуговування. Методи впровадження QoS.

Виявлення пристроїв за допомогою протоколів CDP та LLDP. Протокол NTP. Протокол SNMP. Протокол Syslog. Технічне обслуговування файлових систем маршрутизаторів та комутаторів. Керування образами IOS.
Мережева документація. Методика пошуку та усунення несправностей. Інструменти для пошуку та усунення несправностей. Ознаки та причини проблем з мережею.

5.2. Структура навчальної дисципліни

Денна форма навчання

Назви змістових модулів і тем	Кількість годин					
	Форма навчання: денна					
	Усього	у тому числі				
		лекції	практичні (семінарські)	лабораторні	індивідуальна робота	самостійна робота
Модуль 1						
Тема 1. Вступ. Основи мережевого з'єднання та передавання даних.	10			2		8
Тема 2. Еталонні моделі OSI та TCP/IP.	10	2				8
Тема 3. Ethernet-концепції.	12			4		8
Тема 4. Поняття комутації. Обладнання комутації, VLAN.	10	2				8
Тема 5. Поняття маршрутизації. Обладнання маршрутизації, маршрутизація між VLAN.	12	2		2		8
Тема 6. Безпека на 2 рівні моделі OSI та WLAN.	4	2		2		
Модульна контрольна робота	2	2				
Разом за модуль	60	10		10		40
Модуль 2						
Тема 1. Протоколи динамічної маршрутизації.	14	2		4		8
Тема 2. Налаштування статичної маршрутизації.	10			2		8
Тема 3. Безпека на 3 рівні моделі OSI.	14	2		4		8
Тема 4. Резервування комунікаційних мереж.	8	2				6
Тема 5. Оптимізація, контроль та усунення несправностей комунікаційних мереж.	12			4		8
Модульна контрольна робота	2	2				
Разом за модуль	60	8		14		38
Разом за семестр	**120**	**18**		**24**		**78**

5.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість Годин	
		Денна	Заочна
1	Вступне заняття. Базові налаштування комутатора та кінцевого пристрою	2	
2	Підключення фізичного рівня.	2	

3	Використання Wireshark для дослідження кадрів Ethernet.	2	
4	Дослідження MAC-адрес мережевих пристроїв.	2	
5	Реалізація невеликої мережі.	2	
6	Базові налаштування маршрутизатора.	2	
7	Впровадження VLAN та транкових каналів.	2	
8	Налаштування DTP	2	
9	Маршрутизація між VLAN методом Router-on-a-Stick.	2	
10	Усунення несправностей маршрутизації між VLAN	2	
11	Налаштування OSPFv2 для однієї зони	2	
12	Комплексне завдання з розгортання ACL для IPv4	2	
	Разом	**24**	

5.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1.	Організації зі стандартизації мережевих технологій.	4	
2.	Еталонні моделі.	4	
3.	Інкапсуляція та доступ до даних.	4	
4.	Протокол динамічного транкування DTP.	6	
5.	Узгодження режимів інтерфейсів.	4	
6.	Мережі OSPF з множинним доступом.	4	
7.	Поширення маршруту за замовчуванням в OSPF.	4	
8.	Перевірка OSPF для однієї зони.	4	
9.	Інфраструктура віртуальної мережі.	4	
10.	Стандарти бездротових мереж.	4	
11.	Peer-to-peer або Wi-Fi Direct.	4	
12.	Wireless distribution system.	4	
13.	Мережеві екрани ASA.	4	
14.	Забезпечення безпеки з використанням хмарних технологій.	4	
15.	Способи автоматизації мережі.	4	
16.	Кордон безпечного доступу до сервисів (SASE)	4	
17.	Підхід розширеного виявлення та реагування (XDR)	4	
18.	Платформа Cisco Secure	4	
19.	Політика паролів	4	
	Разом	**78**	

6. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Технічні засоби: технічні засоби навчання, зокрема мультимедійний проектор.
Обладнання: персональні комп’ютери з можливістю доступу в Інтернет.
Програмне забезпечення: Cisco Packet Tracer

7. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Киричик Б.М. Аналіз методів підвищення продуктивності комп’ютерної мережі / Б.М. Киричик, Н.Є. Бурак // Захист інформації в інформаційно-комунікаційних системах: Зб. тез доповідей ІІІ Всеукр. наук.- практ. конф. молодих вчених, курсантів та студентів. – Львів: ЛДУ БЖД, 2019. – С. 223-225.

2. 3. Особливості використання засобів Cisco Packet Tracer при вивченні комп'ютерних мереж / Б.І. Іванчук, Н.Є. Бурак // Проблеми та перспективи розвитку системи безпеки життєдіяльності: Зб. наук. праць XV Міжнар. наук.- практ. конф. молодих вчених, курсантів та студентів. – Львів: ЛДУ БЖД, 2020. – С. 201-203.
3. Основи организації мереж Cisco, том 2 [Текст].: Пер. с англ. - М.: Видавництво «Вильямс», 2005. - 215 с.
4. Виткев О. Основи мереж Cisco, том 1. / Виткев О. М.: Видавництво "Вильяме", 2005. – 231 с.

Інформаційні ресурси в мережі Інтернет

1. https://www.cisco.com/c/uk_ua/products/security/index.html
2. https://www.cisco.com/c/ru_ua/solutions/enterprise-networks/enterprise-network-security/index.html