

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
НАВЧАЛЬНА ПРАКТИКА З ОРГАНІЗАЦІЇ, НАЛАГОДЖЕННЯ ТА
ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ
підготовки першого (бакалаврського) рівня вищої освіти
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Кібербезпека та захист інформації

Силабус нормативного освітнього компонента “Навчальна практика організації, з налагодження та захисту комп’ютерних мереж” підготовки бакалавра, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації.

Розробники:

Черняшук Наталія Леонідівна, доктор педагогічних наук, професор, професор кафедри комп’ютерних наук та кібербезпеки

Погоджено

Гарант

освітньо-професійної



програми:

Черняшук Н.Л.

**Силабус освітнього компонента
комп’ютерних наук та кібербезпеки**

затверджено на засіданні кафедри

протокол № 4 від 21.11.2024 р.

Завідувач кафедри:



Гришанович Т. О.

I. Опис освітнього компонента

Найменування показників	12 Інформаційні технології 125 Кібербезпека та захист інформації Кібербезпека та захист інформації бакалавр	Характеристика освітнього компонента
Денна форма навчання	12 Інформаційні технології 125 Кібербезпека та захист інформації Кібербезпека та захист інформації бакалавр	Нормативна
Кількість годин/кредитів 180 / 6		Рік навчання 4
		Семестр 8-ий
		Консультації 12 год.
		Самостійна робота: 168 год
		Форма контролю: залік
Мова навчання: українська		

II Інформація про викладача

ППП: Черняшук Наталія Леонідівна;

Науковий ступінь: доктор педагогічних наук;

Вчене звання: професор;

Посада: професор кафедри комп'ютерних наук та кібербезпеки;

Контактна інформація: Cherniashchuk.Nataliia@vnu.edu.ua

Дні занять: <http://94.130.69.82/cgi-bin/timetable.cgi>

III. Опис практики

1. Анотація практики. Навчальна практика організації, з налагодження та захисту комп'ютерних мереж є складовою навчального плану підготовки бакалаврів спеціальності 125 кібербезпека та захист інформації денної форми навчання. Навчальна практика організації, з налагодження та захисту комп'ютерних мереж, як невід'ємна частина навчального процесу, направлена на закріплення теоретичних знань, які одержані здобувачами в процесі вивчення освітнього компонента Комп'ютерні мережі та орієнтована на проектування комп'ютерної мережі в EVE- NG.

2. Мета і завдання: є отримання практичних навичок з проектування корпоративних комп'ютерних мереж в віртуальній мережевій лабораторії EVE-NG, та вивчення команд операційної системи компанії Cisco Internetwork Operating System (IOS) для конфігурації пристроїв.

Основними задачами навчальної практики з організації, налагодження та захисту комп'ютерних мереж в рамках спеціальності 125 «Кібербезпека та захист інформації», враховуючи ОПП, є наступні:

- здатність розробляти, впроваджувати та супроводжувати системи захисту в інформаційно-телекомунікаційних технологіях;
- вирішувати прикладні і наукові завдання проектування та побудови комплексних систем захисту інформації;

- керувати процесами управління інформаційною та кібербезпекою в різного роду загрозах;
- виконати опис апаратних пристроїв для проектування мережі, їх технічні характеристики;
- виконати розрахунки схеми IP-адресації методом VLSM з урахуванням вимог організації;
- налаштувати маршрутизатори, комутатори і комп'ютери для підтримки з'єднання IPv4;
- налаштувати технологію VLAN;
- налаштувати маршрутизацію між VLAN та між мережами;
- налаштувати DHCP та динамічний NAT;
- представити на перевірку спроектовану комп'ютерну мережу в EVE- NG.

3. Результати навчання.

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК 4. Здатність спілкуватися іноземною мовою.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.

ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

ЗК 8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

СК1. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК2 Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК4. Здатність забезпечувати захист інформації інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)

СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості загрози інформаційному простору інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та або інфраструктури організації в цілому.

РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

IV. ЕТАПИ ПРАКТИКИ

Етапи	Зміст, основні завдання	Конс.	Сам. роб.
Підготовчий	Настановча конференція.	4	15
	Консультація з керівником практики та знайомство із завданнями практики.		
	Розробка індивідуального графіку роботи студента-практиканта.		
Основний	Виконати опис апаратних пристроїв для проектування мережі, їх технічні характеристики/	4	30
	Виконати розрахунки схеми IP-адресації методом VLSM з урахуванням вимог організації.		
	Налаштувати маршрутизатори, комутатори і комп'ютери для підтримки з'єднання IPv4.		30
	Налаштувати технологію VLAN.		

	Налаштувати маршрутизацію між VLAN та між мережами.		30
	Налаштувати DHCP та динамічний NAT.		
	Представити на перевірку спроектовану комп'ютерну мережу в EVE- NG.		15
Підсумковий	Узагальнення та систематизація матеріалу щодо проходження навчальної практики. Підготовка звітної документації.	4	15
	Оформлення звіту про практику за поданим зразком.		10
	Представлення звіту про практику та його затвердження.		10
	Захист практики.		13
Всього		12	168

V. ВИДИ (ФОРМИ) ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

Кожен здобувач в якості індивідуального завдання повинен виконати всі етапи проходження практики.

VI. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ПРАКТИКИ

Зміст роботи, що оцінюється	Кількість балів
1. Теоретична підготовка: - виконати опис апаратних пристроїв для проектування мережі, їх технічні характеристики;/; - виконати розрахунки схеми IP-адресації методом VLSM з урахуванням вимог організації.- вміння обирати кольори, шрифти при проектуванні інтерфесів.	25
2. Практична підготовка: - налаштувати маршрутизатори, комутатори і комп'ютери для підтримки з'єднання IPv4; - налаштувати технологію VLAN; - налаштувати маршрутизацію між VLAN та між мережами; - налаштувати DHCP та динамічний NAT; - представити на перевірку спроектовану комп'ютерну мережу в EVE- NG.	55
3. Особистісні характеристики: – дисциплінованість під час проходження практики; – ініціативність; – самостійність; – професійна спрямованість; – вчасність виконання завдань.	10
4. Оцінювання звітної документації: – підготовка звіту практики.	10
Сума	100

Політика оцінювання

Політика викладача щодо здобувача освіти

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загально-прийнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності.

Проходження практики передбачає відвідування студентами настановчої конференції перед початком практики, де вони отримують завдання. Поставити питання для керівника практики, уточнити завдання, з'ясувати незрозумілі моменти здобувачі освіти можуть на консультаціях, які проводяться керівником практики відповідно до графіку. Кожен здобувач повинен бути учасником дистанційного курсу "Навчальна практика з організації, налагодження та захисту комп'ютерних мереж". Передбачено спілкування керівника практики зі здобувачами через форум дистанційного курсу. До захисту практики допускаються здобувачі, які виконали завдання, оформили звіт практики та завантажили відповідну документацію до дистанційного курсу. Вимоги до звіту та приклад його оформлення здобувачі можуть переглянути на дистанційному курсі.

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.

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); посилення 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.

Політика щодо дедлайнів та перескладання

Навчальна практика з організації, налагодження та захисту комп'ютерних мереж триває протягом семестру. Терміни практики оголошуються керівником практики на настановчій конференції, зазначаються у дистанційному курсі. Матеріали практики, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. У випадку, коли здобувач освіти не виконав завдання практики у зазначені терміни, він має можливість виконати завдання під час ліквідації академічної заборгованості.

VI. Шкала оцінювання

Оцінка в балах за всі види навчальної діяльності	Оцінка
90–100	Зараховано
82–89	
75–81	
67–74	
60–66	
1–59	Незараховано (з можливістю повторного складання)

V. Підсумковий контроль

Підсумковою формою контролю є залік. Оцінювання навчальних досягнень здійснюється за 100 бальною шкалою. Оцінювання здійснюється на основі представленого звіту, захисту матеріалів практики, що відбувається за присутності усіх студентів-практикантів та керівника практики.

Якщо за результатами виконання завдань накопичено не менше 60 балів і студент погоджується із цим результатом, то виставляється оцінка за семестр. В іншому випадку здобувач освіти має можливість скласти залік під час ліквідації академічної заборгованості.

Ліквідація академічної заборгованості із практики передбачає виконання того ж набору індивідуальних задач із подальшим захистом результатів практики.

VI. Рекомендована література та інтернет-ресурси.

1. Положення про організацію освітнього процесу Волинського національного університету імені Лесі Українки, затверджене Вченою радою Волинського національного університету імені Лесі Українки 29 серпня 2024 року <https://ed.vnu.edu.ua/71-2/нормативні-документи-вну-імені-лесі-у/>

2. Положення про проведення практики здобувачів освіти Волинського національного університету імені Лесі Українки затверджене Вченою радою Волинського національного університету імені Лесі Українки 29 серпня 2024 року <https://ed.vnu.edu.ua/71-2/нормативні-документи-вну-імені-лесі-у/>

3. Освітньо-професійна програма вищої освіти «Кібербезпека та захист інформації» <https://vnu.edu.ua/uk/faculties/fakultet-informatsiynykh-tekhnohoy-i-matematyky>

4. Інструкція із питань охорони праці та безпеки життєдіяльності для учасників освітнього процесу (студентів) під час навчання у Волинському національному університеті імені Лесі Українки <https://drive.google.com/file/d/122CaJMQm5h32PZ20FgeGAHq-9r9mbueq/view>