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 F5 Кібербезпека та захист інформації
освітньо-професійної програми Кібербезпека та захист інформації

Луцьк – 2025

Силабус нормативного освітнього компонента “Навчальна практика організації, з налагодження та захисту комп’ютерних мереж” підготовки бакалавра, галузі знань F Інформаційні технології, спеціальності F5 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації.

Розробники:
Чернящук Наталія Леонідівна, доктор педагогічних наук, професор, професор кафедри комп’ютерних наук та кібербезпеки

Погоджено
Гарант освітньо-професійної програми: Чернящук Н.Л.

Силабус освітнього компонента затверджено на засіданні кафедри комп’ютерних наук та кібербезпеки
протокол № 2 від 17.09.2025 р.

Завідувач кафедри: Гришанович Т. О.

І. Опис освітнього компонента

<table>
<tr><td>Найменування показників</td><td>F Інформаційні технології
F5 Кібербезпека та захист інформації
Кібербезпека та захист інформації
бакалавр</td><td>Характеристика освітнього компонента</td></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="5"></td><td>Нормативна</td></tr>
<tr><td>Рік навчання 4</td></tr>
<tr><td rowspan="4">Кількість годин/кредитів 180 / 6</td><td>Семестр 8-ий</td></tr>
<tr><td>Консультації 12 год.</td></tr>
<tr><td>Самостійна робота: 168 год</td></tr>
<tr><td>Форма контролю: залік</td></tr>
<tr><td colspan="2">Мова навчання: українська</td><td></td></tr>
</table>

ІІ Інформація про викладача

ПІП: Чернящук 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

ІІІ. Опис практики

Анотація практики. Навчальна практика організації, з налагодження та захисту комп'ютерних мереж є складовою навчального плану підготовки бакалаврів спеціальності F5 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.

Пререквізити: комп'ютерні мережі, операційні системи, основи інформаційної безпеки, адміністрування мережевих систем, криптографічний захист інформації.

Постреквізити: проєктування захищених мережевих систем, кіберзахист інформаційно-комунікаційних систем, аудит інформаційної безпеки, практична підготовка (виробнича практика).

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 загроз;

– 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.

Компетентності. Програмні результати навчання. Soft skills.

ЗК1. Здатність застосовувати знання у практичних ситуаціях

ЗК2. Знання та розуміння предметної області і 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.

ЗК6. 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.

ЗК7. 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.)

СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною 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.

Комунікація – вміння чітко пояснювати технічні аспекти мережевих рішень колегам та керівництву.

Командна робота – ефективна взаємодія в групі під час виконання практичних завдань і проєктів.

Проблемне мислення – здатність аналізувати проблеми, швидко знаходити причини збоїв і пропонувати рішення.

Управління часом – планування робочого процесу, дотримання термінів виконання завдань.

Адаптивність – здатність швидко опановувати нові технології, підлаштовуватись під зміни у проєктних вимогах.

Прийняття рішень – оцінка ризиків та вибір оптимальних методів налагодження і захисту мереж.

Критичне мислення – аналіз інформації та оцінка ефективності заходів безпеки.

Відповідальність і дисципліна – дотримання правил безпеки, політик та регламентів роботи з інформаційними системами.

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 проєкутванні 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

IV. Політика оцінювання

Політика викладача щодо здобувача освіти

Усі учасники освітнього процесу зобов'язані дотримуватись вимог чинного законодавства України, Статуту та Правил внутрішнього розпорядку Волинського національного університету імені Лесі Українки, а також загальноприйнятих норм академічної етики, корпоративної культури та взаємоповаги.
Під час занять підтримується атмосфера співпраці, відкритості, відповідальності й толерантності. Очікується активна участь студентів у лекційних і лабораторних заняттях, своєчасне виконання індивідуальних та групових завдань, дотримання графіка навчання та вимог до оформлення робіт. Недопустимими є запізнення, використання мобільних пристроїв не за навчальним призначенням, плагіат, списування, підміна особи та будь-які прояви порушення академічної доброчесності. Усі лабораторні, самостійні й підсумкові завдання виконуються із використанням засобів дистанційного курсу дисципліни в системі Moodle.
Викладач гарантує прозорість та об'єктивність оцінювання, надання зворотного зв'язку, створення комфортних умов для засвоєння матеріалу й розвитку професійних і комунікаційних компетентностей здобувачів освіти.

Політика щодо академічної доброчесності.

Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно, а результати раніше зданих робіт анулюються і виконуються повторно у порядку визначеному викладачем. При цьому викладач залишає за собою право змінити завдання.

Політика дедлайнів та перескладання.

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).

Можливість визнання результатів навчання, отриманих у формальній, неформальній та інформальній освіті.

Під час вивчення освітнього компонента можливе визнання результатів навчання отриманих у формальній, неформальній та/або інформальній освіті. Порядок визнання результатів навчання для здобувачів вищої освіти, набутих у: формальній освіті (академічна мобільність студентів на території України чи поза її межами, для студентів, які переводяться, поновлюються з інших ЗВО (вітчизняних чи іноземних); неформальній та/або інформальній освіті здійснюється згідно «ПОЛОЖЕННЯ про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки».

Можливість отримати додаткові бали.

Здобувачі освіти можуть отримувати додаткові бали за активну участь у навчальній практиці, своєчасне та якісне виконання практичних і самостійних завдань, прояв ініціативи під час обговорень, а також за виконання завдань підвищеної складності.

Додаткові бали можуть нараховуватися за: участь у науково-дослідній діяльності, конференціях, олімпіадах або конкурсах з питань інформаційної безпеки; розробку власних мініпроєктів або практичних рішень з налагодження та захисту мереж; створення навчальних матеріалів, презентацій або довідників для одногрупників; відвідування всіх занять практики та активну участь у виконанні практичних завдань.

Нарахування додаткових балів здійснюється відповідно до встановлених критеріїв оцінювання та не може перевищувати граничне значення, визначене системою оцінювання навчальної практики.

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 70 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. Шкала оцінювання

Оцінка в балах	Лінгвістична оцінка
90–100	Зараховано
82–89	
75–81	
67–74	
60–66	
0–59	Незараховано (необхідне перескладання)

VI. Рекомендована література та інтернет-ресурси.

1. ДСТУ 3008-2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – К.: Держстандарт, 2015. – 37 с. 2.
2. 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/
3. 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/
4. Освітньо-професійна програма вищої освіти «Кібербезпека та захист інформації» https://vnu.edu.ua/uk/faculties/fakultet-informatsiynykh-tekhnolohiy-i-matematyky
5. 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