Волинський національний університет імені Лесі Українки
Кафедра комп'ютерних наук та кібербезпеки
СИЛАБУС
Практика з організації, налагодження та захисту інформації

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Освітня програма	Кібербезпека та захист інформації
Форма навчання	Денна
Розробник	Глинчук Людмила Ярославівна, к. фіз.-мат. наук;
Контактна інформація	hlynchuk.ludmila@vnu.edu.ua
Семестр, курс	4 курс, 7 семестр
Обсяг дисципліни	Загальний обсяг: 180 годин, 6 кредити Самостійна робота: 168 годин Консультації: 12 год.
Форма контролю	Залік
Час занять	2-16 тижні
Мова навчання	Українська
Анотація дисципліни	Підготовка закладами вищої освіти фахівців спеціальностей 125 Кібербезпека та захист інформації передбачає обов'язкову практичну підготовку, що реалізується під час організації та проведення практики, яка здійснюється з метою закріплення теоретичних знань, ознайомлення з майбутньою професією, набуття досвіду самостійної роботи та набуття виробничих навиків приймати самостійно рішення. Практика з організації, налагодження та захисту інформації є невід'ємною складовою частиною процесу професійної підготовки здобувачів, які навчаються за освітньою програмою Кібербезпека та захист інформації і проводиться в навчально- науковій лабораторії захисту інформації, яка оснащена відповідним апаратним та програмним забезпеченням. Практика передбачає самостійну діяльність здобувача з поглиблення і закріплення теоретичних знань з захисту інформації в комп'ютерних мережах, спрямована на розвиток у студентів умінь та навичок проектувати комп'ютерну мережу та організовувати захист інформації вмережі.
Мета вивчення дисципліни	Метою даної дисципліни є формування у здобувачів навичок самостійної роботи, уміння використовувати теоретичні знання в конкретних видах діяльності, надбання у здобувачів під час практики умінь та навичок самостійного розв'язання завдань, пов'язаних з використанням спеціалізованого апаратного та програмного забезпечення в своїй роботі. Під час проходження практики здобувачі повинні навчитись виконувати адміністрування прав доступу до комп'ютерної системи та мережі з метою перешкоди призначення невиправданих привілеїв, підбирати тип та структуру локальної комп'ютерної мережі.
Що буде вивчатися	Знайомство з правилами внутрішнього розпорядку інструктаж з техніки безпеки та охорони праці. Ознайомлення з технічними характеристиками навчально-наукової лабораторії захисту

	інформації. Загальна схема проектування корпоративної мережі. Основні задачі оптимізації мереж. Особливості створення функціональної моделі. Cisco Packet Tracer. Серверна операційна система на базі ОС Linux. Налагодження і оптимізація роботи системного та прикладного програмного забезпечення на серверах і робочих станціях. Організація віддаленого доступу. Проведення профілактичних робіт по обслуговуванню програмного і апаратного забезпечення. Розмежування прав доступу користувачів до загальних ресурсів комп'ютерів в мережі. Впровадження систем антивірусного захисту. Використання хмарної платформи забезпечення захисту Cisco Umbrella. Використання та налагодження пристроїв: апаратний міжмережевий екран для мереж фаєрвол Cisco ASA5506-X; комутатор MikroTik CRS125-24G-1S-IM; маршутизатор Mikrotik RB4011iGS+5HacQ2HnD-IN; маршрутизатор MikroTik RouterBOARD.
Результати навчання	**Загальні компетенції** **ЗК 1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК 2.** Знання та розуміння предметної області та розуміння професії. **ЗК 3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **ЗК 4.** Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **ЗК 5.** Здатність до пошуку, оброблення та аналізу інформації. **Фахові компетенції** **ФК 5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. **ФК 12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. **Програмні результати навчання** **ПРН 2.** Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. **ПРН 3.** Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. **ПРН 4.** Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. **ПРН 5.** Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

	ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. **ПРН 7.** Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки. **ПРН 11.** Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. **ПРН 14.** Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень. **ПРН 15.** Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. **ПРН 17.** Забезпечувати процеси захисту та функціонування інформаційнотелекомунікаційних автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. **ПРН 18.** Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. **ПРН 21.** Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах.

Політика щодо академічної доброчесності

Дотримання здобувачами вищої освіти академічної доброчесності при виконанні індивідуального завдання виробничої практики та оформленні звіту практики регламентується ст. 42 Закону України «Про освіту», Кодексу академічної доброчесності Волинського національного університету імені Лесі Українки, Положенням про систему запобігання та виявлення академічного плагіату у науково-дослідній діяльності здобувачів вищої освіти і науково-педагогічних працівників ВНУ імені Лесі Українки.

У разі виявлення керівником практики від факультету у роботі здобувача вищої освіти одного або кількох видів порушень академічної доброчесності, а саме: академічного плагіату, самоплагіату, фабрикації, фальсифікації, обману, здобувач вищої освіти до захисту практики не допускається, до нього можуть бути застосовані види відповідальності, передбачені Кодексом академічної доброчесності Волинського національного університету імені Лесі Українки, зокрема: повторне проходження оцінювання; повторне проходження відповідного освітнього компонента освітньої програми; відрахування з університету; позбавлення академічної стипендії; позбавлення наданих університетом пільг з оплати навчання.

Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану адресу електронної пошти, що надається університетом. Комунікація між викладачем та здобувачем освіти здійснюється виключно із використанням корпоративних засобів комунікації. Також можливе інше (додаткове) джерело комунікації, визначене викладачем для більш оперативного зв'язку зі студентами.

Форми звітності при проходженні практики

Формами звітності проходження технологічної практики є комплексний щоденник

практик та письмовий звіт, оформлені згідно вимог.

Форми і методи контролю

До видів контролю виконання завдань технологічної практики відносяться:

- контроль за вчасним проведенням робіт, що зазначені у індивідуальному завданні та календарному плані технологічної практики;
- вчасне надання керівнику матеріалів технологічної практики відповідно до індивідуального завдання;
- контроль за якістю підготовки студентом письмового звіту про виконання завдань технологічної практики;
- контроль за вчасним поданням керівнику на перевірку письмового звіту про виконання завдань технологічної практики;
- контроль за підготовкою студента до захисту на кафедрі результатів технологічної практики згідно вимог індивідуального завдання.

Критерії оцінювання практики

Допуск студента до захисту технологічної практики здійснює керівник практики від кафедри. Критерієм допуску є:

- наявність заповненого щоденника практики;
- наявність письмового звіту про виконання завдань технологічної практики, з дотриманням всіх вимог та завіреного керівником бази практики;
- відповідність змісту звіту темі індивідуального завдання.

Результати проходження практики та звіт студентів обговорюються на публічному захисті практики в присутності комісії, затвердженої наказом на практику, та керівника практики від кафедри. Захист практики організовується протягом перших 10 днів семестру, який починається після завершення практики.

Комісія приймає залік у терміни, що визначені наказом на практику.

Оцінювання результатів проходження технологічної практики відбувається на комісії.

Критерії оцінювання:

Зміст роботи, що оцінюється	**Кількість балів**
1. Техніка безпеки і охорона праці на об'єкті практики: Знайомство з правилами внутрішнього розпорядку, інструктаж з техніки безпеки та охорони праці.	10
2. Загальні відомості про об'єкт практики Ознайомлення з апаратним та програмним забезпеченням навчально-наукової лабораторії захисту інформації. Відображення результатів в звіті практики.	10
3. Виконання індивідуальних завдань практики.	30
4. Виконання обов'язків згідно з місцем проходження практики в університеті: Ознайомлення з обов'язками фахівця з захисту інформації. Робота зі стандартним обладнанням та програмним забезпеченням. Робота в середовищі сучасних операційних систем та баз даних. Налаштування обладнання телекомунікаційних систем та мереж, апаратних, програмних, локальних та мережевих засобів. Аналіз роботоспроможності мережі та пошук в них уразливостей за допомогою спеціального програмного забезпечення.	30
5. Підготовка і оформлення звітних матеріалів та захист практики Узагальнення та систематизація матеріалу щодо проходження технологічної практики. Підготовка необхідної документації. Оформлення пояснювальної записки звіту з технологічної практики.	20
Сума	100

Диференційована оцінка за технологічну практику вноситься в відомість, індивідуальний навчальний план (залікову книжку) студента за підписами членів комісії і

враховується під час визначення розміру стипендій разом з іншими підсумковими оцінками. У разі отримання незадовільної оцінки під час складання заліку студенту надається можливість повторного складання заліку за умови доопрацювання звіту й індивідуального завдання. За умови отримання незадовільної оцінки з практики під час ліквідації заборгованості комісії студент відраховується з університету.

Рекомендована література та інтернет-ресурси

1. Положення про проведення практики студентів Волинського національного університет імені Лесі Українки [Електронний ресурс] — Режим доступу : https://vnu.edu.ua/uk/normativno-pravova-baza
2. Закон України «Про вищу освіту», Указ президента України від 04.07.2005р. №1013/2005 «Про невідкладні заходи щодо забезпечення функціонування та розвитку освіти в Україні».
3. Положення про навчання у Волинському національному університеті імені Лесі Українки для здобуття першого (бакалаврського) ступеня на основі раніше здобутих освітньо-кваліфікаційного рівня «молодший спеціаліст», освітнього ступеня «фаховий молодший бакалавр» [Електронний ресурс] — Режим доступу : https://vnu.edu.ua/uk/normativno-pravova-baza
4. Положення про проведення практики студентів вищих навчальних закладів України Електронний ресурс] — Режим доступу : https://zakon.rada.gov.ua/laws/show/z0035-93#Text
5. Захист інформації в комп'ютерних системах: підручник / В. Д. Козюра, В.О. Хорошко, М. Є. Шелест, Ю. М Ткач, О.О.Балюнов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.
6. Інформаційна безпека в комп'ютерних мережах : навч. посіб. / О. А. Смірнов, О. К. Конопліцька-Слободенюк, С. А. Смірнов [та ін.] ; М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т. - Кропивницький : Лисенко В.Ф., 2020. – 295 с.

Затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки
протокол № 2 від 28.09.2023р.

Завідувач кафедри:  (Гришанович Т. О.)