Волинський національний університет імені Лесі Українки
Кафедра комп'ютерних наук та кібербезпеки
СИЛАБУС
Дисципліни професійної підготовки
Виробнича практика з організації 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	3 курс, 6 семестр
Обсяг дисципліни	Загальний обсяг: 180 годин, 6 кредитів Самостійна робота: 168 годин Консультації: 12 год.
Форма контролю	Залік
Мова навчання	Українська
Анотація дисципліни	Виробнича практика з організації захисту інформації студентів, які набувають кваліфікаційний рівень бакалавра за спеціальністю 125 Кібербезпека та захист інформації, є невід'ємною складовою навчального процесу. Під час практики студенти мають набути навичок експлуатації та захисту комп'ютерних систем та мереж, що спрямовано на практичну підготовку до самостійної роботи із розв'язання практичних завдань на підприємстві. Виробничу практику студенти проходять на підприємствах різних форм власності під керівництвом викладачів кафедри і працівників відповідних підприємств. Така організація керівництва практикою дає змогу студентам поглибити теоретичні знання і набути досвіду практичної роботи. Під час практики з організації захисту інформації студенти збирають необхідну інформацію про господарську діяльність підприємства та її результати, здійснюють аналіз результатів діяльності підприємства і визначають наявність проблем. У разі виявлення на підприємстві проблем студенти повинні вказати можливі шляхи їх вирішення. Результати роботи студенти оформлюють у вигляді звіту з практики. Оцінюють результати роботи студентів спочатку керівники практики від університету та підприємства у вигляді відгуку, а потім комісія із захисту практики.
Мета вивчення дисципліни	Метою даної дисципліни є закріпити і поглибити знання, отримані за час навчання в університеті, і використовувати їх для обґрунтованого прийняття проектних рішень, набути досвіду роботи виконання пошуку і порівняльного аналізу при виборі найбільш прийнятних протоколів, алгоритмів та програм, вдосконалити знання й уміння при проектуванні систем в цілому і практично закріпити навички розробки її базових елементів програмного, інформаційного та технічного забезпечення для комплексів автоматизованого проектування, інформаційно-пошукових систем, комп'ютерних мереж, системи дистанційного навчання, набути досвіду в

	оформленні проектних і графічних матеріалів, складанні пояснювальних записок, специфікацій, відомостей на програмне забезпечення. Під час проходження практики студенти повинні вивчити організаційну структуру підприємства; ознайомитись зі звітними та іншими інформаційними документами про діяльність підприємства; навчитись приймати управлінські рішення в реальних ситуаціях, які виникають у поточній діяльності підприємства (установи).
Що буде вивчатися	- Техніка безпеки і охорона праці на об'єкті практики. Знайомство з правилами внутрішнього розпорядку підприємства, інструктаж з техніки безпеки та охорони праці, бесіда спеціалістів. Техніка безпеки і охорона праці у підрозділі. Техніка безпеки і охорона праці на робочих місцях. - Знайомство з підприємством. Екскурсія по відділам підприємства та службам, що забезпечують його роботу. Вивчення роботи основних структурних підрозділів, особливостей роботи окремого структурного підрозділу. Ознайомлення з обчислювальним центром підприємства; з підрозділами підприємства; з обов'язками згідно з місцем роботи у підрозділі підприємства; з обов'язками фахівця з захисту інформації. Практиканти повинні проаналізувати рівень комп'ютерного забезпечення підприємства (установи): кількість серверів, персональних комп'ютерів, ноутбуків, інших обчислювальних пристроїв, особливості їх архітектури, апаратну конфігурацію, інтерфейси та ін. Далі проводиться аналіз периферійного (пристрої вводу-виводу, їх функціональні характеристики) та мережевого обладнання (маршрутизатори, комутатори, wifi-роутери, модеми, тощо), локальної комп'ютерної мережі бази практики (топологія, передавальне середовище, тип підключення до глобальної комп'ютерної мережі Internet) та ін. - Робота зі стандартним обладнанням та програмним забезпеченням. Робота в середовищі сучасних операційних систем та баз даних. Налаштування обладнання комп'ютерних систем та мереж, апаратних, програмних, локальних та мережевих засобів. Робота дублером адміністратора комп'ютерних систем та мереж. Обслуговування засобів комп'ютерних систем та мереж. Аналіз роботоспроможності мережі та пошук в них вразливостейй за допомогою спеціального програмного забезпечення. Робота дублером ремонтника апаратних засобів комп'ютерних систем та мереж. Аналіз апаратних засобів комп'ютерних систем та мереж. Аналіз апаратних засобів комп'ютерних систем та мереж спеціальним програмним забезпеченням. Аналіз вразливостей комп'ютерних систем та мереж. Оцінка вразливостей в комп'ютерних системах та мережах. Вивчення наукових розробок в напрямку виявлених вразливостей на підприємстві. Використовування електронної пошти та телеконференцій для спілкування. Вивчення впровадження нових моделей базових захисту інформаційних процесів та висунення пропозицій щодо оптимізації, удосконалення та розвитку існуючих.

Результати навчання	**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. **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 і свобод людини і громадянина в Україні. **ЗК 7.** 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. **ФК 1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. **ФК 2.** Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. **ФК 3.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **ФК 4.** Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики безпеки. **ФК 5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. **ФК 6.** Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. **ФК 7.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). **ФК 8.** Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **ФК 9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою. **ФК 10.** Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. **ФК 11.** Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. **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. **ПРН 40.** Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних- засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. **ПРН 41.** Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. **ПРН 42.** Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. **ПРН 50.** Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). **ПРН 51.** Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. **ПРН 52.** Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. **ПРН 53.** Вирішувати задачі аналізу програмного коду на наявність можливих загроз. **ПРН 54.** Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

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. Усі письмові роботи та звіти перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 30%.

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 виробничої практики є комплексний щоденник практик та письмовий звіт, оформлені згідно вимог.

Форми і методи контролю

До видів контролю виконання завдань виробничої практики відносяться:

- контроль за вчасним проведенням робіт, що зазначені у індивідуальному завданні та календарному плані практики;
- вчасне надання керівнику матеріалів практики відповідно до індивідуального завдання;

- контроль за якістю підготовки студентом письмового звіту про виконання завдань практики;
- контроль за вчасним поданням керівнику на перевірку письмового звіту про виконання завдань практики;
- контроль за підготовкою студента до захисту на кафедрі результатів практики згідно вимог індивідуального завдання.

Критерії оцінювання практики

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

- наявність заповненого щоденника практики;
- наявність письмового звіту про виконання завдань виробничої 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 виробничої практики відбувається на комісії.

Критерії оцінювання:

Зміст роботи, що оцінюється	**лькість балів**
Ознайомлення з програмою практики. Знайомство з підприємством, його структурою. Інструктаж з техніки безпеки.	5
Аналіз нормативно-правововового регулювання забезпечення інформаційної (кібербезпеки) безпеки на підприємстві.	5
Аналіз забезпечення комп'ютерною технікою. Периферійне обладнання та комп'ютерна мережа.	10
Аналіз програмного забезпечення комп'ютерної техніки.	10
Аналіз обігу даних та інформації	10
Аналіз основних напрямків забезпечення інформаційної безпеки на підприємстві	15
Аналіз технічного та програмного захисту інформації.	15
Висновки щодо рівня інформаційної безпеки бази практики.	10
Підведення підсумків. Оформлення щоденника, звіту та захист практики.	20
Сума	100

Диференційована оцінка за виробничу 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.
7. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В.Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний, Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178 с
8. Державний стандарт України. ДСТУ 3008-2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання») /[На заміну ДСТУ 3008-95; чинний від 2017-07-01].- Київ: ДП «УкрНДНЦ», 2016. 31 с. URL: http://www.knmu.kharkov.ua/attachments/3659_3008-2015.PDF
9. Державний стандарт України. ДСТУ 8302:2015 "Інформація та документація. Бібліографічне посилання. Загальні вимоги та правила складання" URL:http://lib.npu.edu.ua/files/dstu-8302-2015.pdf
10. Стандарти з інформації, бібліотечної і видавничої справи. URL:http://wwvv.library.univ.kiev.ua/ukr/about/dstu.html
11. ДСТУ ISO 5807:2016 Обробляння інформації. Символи та угоди щодо документації стосовно даних, програм та системних блок-схем, схем мережевих програм та схем системних ресурсів (ISO 5807:1985, IDT).

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

Завідувач кафедри:  (Гришанович Т. О.)