СИЛАБУС ДИСЦИПЛІНИ
«ВИРОБНИЧА ПРАКТИКА»

Ступінь вищої освіти – Бакалавр
Спеціальність 125 – Кібербезпека та захист інформації
Освітня програма «Кібербезпека»
Рік навчання 4, семестр 8
Форма навчання денна
Кількість кредитів ЄКТС 5
Мова викладання українська

Лектор курсу	 **Місюра Максим Дмитрович, к.т.н.** **(портфоліо)**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки, корпус. 15, к. 207, тел. 5278724** **e-mail mdm@nubip.edu.ua**
Сторінка курсу в eLearn	**ЕНК (2 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=5065

ОПИС ДИСЦИПЛІНИ

Програму виробничої практики складено відповідно до освітньо-професійної програми підготовки бакалаврів за спеціальністю 125 «Кібербезпека».

Мета виробничої практики – поєднання теоретичної підготовки здобувачів з формуванням практичних навичок роботи за фахом для полегшення виходу здобувачів на ринок праці після закінчення ЗВО.

Одночасно переслідується і навчальна мета, яка полягає у систематизації, закріпленні і розширенні теоретичних і практичних знань здобувача, набутих в попередні періоди.

Узагальненою метою виробничої практики є закріпити і поглибити знання, отримані за попередній 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 комп'ютерних систем в цілому і практично закріпити навички розробки її базових елементів програмного, інформаційного та технічного забезпечення для комп'ютерних мереж та систем, набути досвіду в оформленні проектних і графічних матеріалів, складанні пояснювальних записок, специфікацій, відомостей та інше.

Місце і роль дисципліни в системі підготовки фахівців відповідно до навчального плану. Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ1 Здатність застосовувати знання у практичних ситуаціях.

КЗ2 Знання та розуміння предметної області та розуміння професії.

КЗ3 Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

КЗ4 Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ5 Здатність до пошуку, оброблення та аналізу інформації.

Спеціальні (фахові) компетентності:

СК1 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.

СК3 Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК4 Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

СК6 Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних

(автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

СК7 Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме

ПРН3 Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН4 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.

ПРН20 Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнувальних програмних впливів, руйнувальних кодів в інформаційно-телекомунікаційних системах.

ПРН21 Вирішувати задачі забезпечення та супроводу (в тому числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН22 Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

СТРУКТУРА КУРСУ

№ з/п	Етапи проходження практики та види діяльності студентів	Всього годин
1. Організаційний етап. Розробка планів і ознайомлення зі змістом практики		
1.	Організаційні заходи щодо проходження практики, ознайомлення з програмою, завданням, формами звітності з практики	5

2.	Розробка планів і визначення змісту практики	5
	Разом	**10**
2. Виконання завданнь за планом практики		
3.	Виконання програми виробничої практики за індивідуальним планом	120
	Разом	**120**
3. Підсумки виробничої практики		
4.	Підготовка звітних матеріалів про проходження виробничої практики	10
5.	Захист студентом виробничої практики	10
	Разом	**20**
	Всього годин	**150**

ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів та перескладання:	Дедлайни визначені в ЕНК. 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, стажування або відрядження).
Політика щодо академічної доброчесності:	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням комп'ютерної техніки, мобільних пристроїв).
Політика щодо відвідування:	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету).

ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзаменів	**Заліків**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. ДСТУ 3008-95 Документація. Звіти у сфері науки і техніки. Структура і правила оформлення.
2. Николайчук Я.М., Возна Н.Я., Пітух І.Р. Проектування спеціалізованих комп'ютерних систем / Навчальний посібник / - Тернопіль: ТзОВ "Терно граф". 2010. – 392с., іл.
3. Николайчук Я.М., Пітух І.Р., Возна Н.Я. Теорія моделей руху даних розподілених комп'ютерних систем / Монографія - Тернопіль: ТзОВ "Терно граф", 2008 – 216 с..
4. ДСТУ 2396-94 Системи оброблення інформації. Теорія інформації. Терміни та визначення
5. ДСТУ 2481-94 Системи оброблення інформації. Інтелектуальні інформаційні технології. Терміни та визначення
6. ДСТУ 2482-94 Системи оброблення інформації. Комп'ютерні технології навчання. Терміни та визначення
7. ДСТУ/ISO/IEC 2382-32-2003 Інформаційні технології. Словник термінів. Частина 32. Електронна пошта (ISO 2382-32-2003)
8. Закон України «Про інформацію» від 02.10.1992 № 2657-XII
9. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
10. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373
11. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
12. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
13. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
14. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу
15. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
16. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2
17. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу
18. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
19. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу
20. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.