Форма №Н-3.04

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"__" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол №10 від "17" травня 2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»
_____
Гарант ОП
_____ (проф. Лахно В.А.)

РОБОЧА ПРОГРАМА
Виробнича практика

Спеціальність	125 «Кібербезпека»
Освітня програма	«Кібербезпека»
Факультет	інформаційних технологій
Розробник:	Місюра М.Д., к.т.н.

Київ – 2023р.

ВСТУП

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

1. Опис виробничої практики

1.1. Мета виробничої практики

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.

1.2. Основні завдання виробничої практики:

• вивчити техніко-економічні умови діяльності підприємства, установи, організації (баз практик), їх фінансового стану;

• ознайомитися з організацією роботи на базах практики;

• набути навичок практичного застосування теоретичних знань для розв'язання завдань надання послуг з захисту інформації;

• навчитися аналізувати та прогнозувати результати, планувати заходи та приймати управлінські рішення щодо поліпшення технічного та технологічного стану підприємства;

• ознайомитися із структурою підприємства чи установи;

• вивчити установчі документи та ознайомитися з положеннями про відділи, посадовими інструкціями, взаємовідносинами між структурними підрозділами, технологією управління ресурсами на базі практики;

• вивчення нормативної бази, що регулює забезпечення інформаційної безпеки і захисту інформації, що використовується та обробляється даним підприємством;

• узагальнення, закріплення і поглиблення знань, що отримані під час навчання в ЗВО для використання їх у подальшій роботі та обґрунтованого прийняття рішень;

• ознайомлення з засобами забезпечення інформаційної безпеки і захисту інформації, що використовуються підприємством;

• отримання інформації про те, які знання, отримані у ЗВО, і в якому напрямі необхідно поглиблювати і розвивати;

• знайомство з новими технологіями в ІТ- індустрії.

• взяти участь у виконанні конкретної роботи, що здійснюється технічними службами підприємства;

• підготувати пропозиції щодо поліпшення організації управління підприємства чи установи;

• опрацювання наукової, періодичної літератури й методичних матеріалів з питань, що підлягають опрацюванню.

• підготувати та захистити звіт за результатами проходження виробничої практики.

1.3. Характеристика виробничої практики

Найменування пказників	Характеристика за показинками	
	Денна	заочна
Вид практики	Виробнича	
Загальний обсяг: години/кредити	150/5	
Курс	3	
Семестр	6	
Кількість змістових компонентів	3	
Тривалість	6 тижнів	
Форма семестрового контролю	Залік	

1.4. Заплановані результати виробничої практики

Набуття компетентностей.

Відповідно до освітньої програми підготовки фахівців за спеціальністю 123 «Комп'ютерна інженерія» виробнича практика 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, предметні) компетентності (СК):

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.).

У 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.

2. Зміст та організація виробничої практики

Виробнича практика є обов'язковою формою поглибленого навчання в системі підготовки фахівців за ступенем вищої освіти «бакалавр».

Зміст виробничої практики повинен забезпечувати виконання мети і всіх завдань програми підготовки бакалаврів. Перед початком практики здобувач отримує індивідуальне завдання на період практики, яке підписується здобувачем і керівником практики. Основні завдання практики відображаються в індивідуальному графіку. Під час практики здобувач повинен ознайомитись з проблемою створення та використання сучасних комп'ютерних систем, які використовуються в організації за місцем практики, ознайомитись з мовами програмування та пакетами програм, які використовуються, ознайомитися з інформаційними та Інтернет-технологіями.

Згідно отриманого індивідуального завдання здобувач повинен розробити комплект документації, відповідно до поставленого завдання.

Зміст виробничої практики:

№ 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**

І тиждень

Ознайомлення з виробничими умовами за місцем практики. Прибуття на місце практики. Знайомство з керівником практики на підприємстві. Проходження інструктажів з правил техніки безпеки на робочому місці. Знайомство з конкретними умовами і змістом роботи персоналу та посадовими обов'язками співробітників у галузі інформаційних технологій. Знайомство з варіантами навчально-виробничих завдань, які пропонуються на період практики. Вивчення запропонованої керівником документації (вимоги, стандарти,

звіти), які можуть бути необхідні або корисні при виконанні навчально-виробничих завдань. Остаточний вибір за участю керівника варіанту навчально-виробничого ознайомчого завдання, документування його змісту, виданих рекомендацій та форм звітності. Складання плану роботи над завданням і затвердження його керівником. Початок ведення «Щоденника практики». Виконання навчально-виробничого ознайомчого завдання.

II- III тиждень

Виконання теоретичної частини (розбір статей, інформаційних схем, комп'ютерних програм і відповідної документації, пошук інформації з літератури та Інтернету, складання оглядів і т.п.). Ведення «Щоденника практики».

IV-V тиждень

Виконання практичної частини (розробка комп'ютерних програм або підготовка даних, робота з контрольно-вимірювальною апаратурою, базами даних, участь в тестуванні апаратних або програмних засобів і т.п.). Ведення «Щоденника практики».

VI тиждень

Здача роботи і оформлення звітності. Перевірка керівником якості виконання завдання керівником. Оформлення звітності з навчально-виробничого ознайомчого завдання за вимогами керівника з місця практики. Отримання відгуку керівника з місця практики, оформлення щоденника практики здобувача. Оформлення зведеного звіту про проходження та результати виробничої практики для захисту на кафедрі.

Доповідь про результати практики на конференції з виробничої практики студентів та отримання оцінки за практику.

3. Вимоги до баз виробничої практики

Виробнича практика проводиться на виробничих підприємствах, науково-дослідних і проектно-конструкторських інститутах та установах, інститутах національної академії наук України, закладах вищої освіти відповідного профілю, а також на випускових кафедрах НУБіП України та комерційних виробничо-технічних організаціях і структурах, які проводять науково-технічні роботи або здійснюють розробки і мають здобутки в сфері проблематики кафедри.

Практика може проводитися при наявності відповідного договору між установами та НУБіП України. Студент (здобувач) може з дозволу кафедри самостійно обрати для себе місце проходження практики, якщо вибрана ним база практики безпосередньо відповідає виконанню навчального плану та основним завданням практики. Таке бажання здобувача повинно бути обґрунтованим та підтвердженим відповідною заявою керівнику кафедри і листом з відповідної організації зі згодою про прийняття студента для проходження практики. Зміна бази практики може мати місце лише при наявності поважних причин і може відбуватися лише до подання проекту наказу про проходження практики. Рішення про зміну бази практики приймає завідувач кафедри.

Здобувач не має права самостійно змінювати місце практики. При нез'явленні здобувача на практику без поважних причин, або самостійній зміні місця практики вважається, що студент не виконав навчального навантаження і він може бути відрахованим з університету.

Відповідно обсягу програми підготовки та терміну навчання виробнича практика бакалаврів спеціальності 125 "Кібербезпека" проводиться на 3 курсі. Конкретний період проведення практики визначається наказом по університету.

Керівником практики призначається викладач зі штату кафедри комп'ютерних систем, мереж та кібербезпеки. Він відповідає за організацію та проведення практики.

Керівник практики здійснює контроль за своєчасним і якісним виконанням виданого індивідуального завдання, надає здобувачу методичну допомогу в організації роботи та консультує його щодо тематики завдання.

Навчально-методичне забезпечення здійснює кафедра комп'ютерних систем, мереж та кібербезпеки.

4. Індивідуальні завдання практики

Під час виробничої практики здобувач повинен ознайомитись з проблемою створення та використання сучасних комп‘ютерних систем, які використовуються в організації за місцем практики, ознайомитись з мовами програмування та пакетами програм, які використовуються, ознайомитися з інформаційними та Інтернет-технологіями. Згідно отриманого індивідуального завдання здобувач повинен розробити комплект документації, відповідно до поставленого завдання.

Індивідуальні завдання мають бути складені таким чином, щоб здобувач міг проявити самостійність у вирішенні практичних завдань. Формулювання індивідуального завдання повинно мати спрямованість для вирішення конкретної задачі. Здобувач повинен вміти професійно зробити огляд необхідної наукової та технічної літератури в заданому напрямку, потрібно показати вміння аналізувати та теоретично обґрунтовувати дані, отримані експериментально, після чого на основі отриманих результатів прийняти рішення щодо методів та засобів вирішення поставленої задачі. Матеріали, отримані здобувачем під час виконання індивідуального завдання, можуть в подальшому бути використані для подальшого навчання у наступних курсах, використання в курсових роботах (проектах), підготовки наукових статей, тез доповідей на конференціях та написанні випускової бакалаврської роботи.

5. Вимоги до звіту про виробничу практику

Підсумковий контроль виробничої практики здійснюється після завершення практики. Рішення про успішне виконання програми виробничої практики затверджується на засіданні кафедри на підставі позитивної оцінки керівника практики та вчасного надання здобувачем повного пакету звітної документації.

Основним документом, який свідчить про виконання здобувачем програми виробничої практики є письмовий звіт. Звіт про проходження виробничої практики для захисту на засіданні кафедри повинен точно висвітлювати виконання всіх завдань практики і дозволити перевірити та оцінити якість виконання програми практики. Звіт повинен мати чітку, логічну і послідовну структуру, переконливу аргументацію, обґрунтованість та висновки.

Зміст звіту повинен розкривати уміння та знання студента, набуті ним на виробничій практиці. Звіт складається індивідуально кожним здобувачем. Оформлення звіту проводиться відповідно до ДСТУ 3008-95. Звіти у сфері науки і техніки. Звіт виконується державною мовою з дотриманням орфографії та стилістики.

При завершенні виробничої практики здобувач повинен здати керівникові практики звіт з виробничої практики та щоденник практики.

6. Підбиття підсумків виробничої практики

Оформлений звіт і заповнений щоденник практики здобувач подає на перевірку керівнику практики від підприємства (організації, установи). При позитивній оцінці він підписує щоденник і робить в ньому запис, що звіт перевірено і позитивно оцінено, та пише характеристику-відгук на здобувача, в якій оцінює рівень виконання програми практики і оформлення звіту.

В останній день практики здобувач подає звіт, щоденник та характеристику керівнику практики від кафедри комп’ютерних систем, мереж та кібербезпеки для перевірки. При виявлені невиконаних робіт або невідповідності встановленим вимогам, звіт повертається здобувачу на доопрацювання. За результатами перевірки керівник практики від кафедри визначає оцінку, за якою звіт рекомендується до захисту. Ця оцінка є рекомендаційною та не є обов‘язковою. Оцінка визначається з урахуванням своєчасності подання документів з практики, якості звіту, рівня знань та рівня захисту здобувача. Оцінка виставляється відповідно до критеріїв та заноситься в заліково-екзаменаційну відомість та залікову книжку та враховується при визначені стипендії разом з оцінками за результатами підсумкового семестрового контролю.

При відсутності звіту чи інших обов‘язкових документів, або отриманні незадовільної оцінки при захисті результатів практики здобувач рекомендується до відрахування з університету. Підсумки практики виносяться на обговорення на засідання кафедри.

7. Методи контролю та схема нарахування балів

Контроль діяльності здобувачів під час виробничої практики здійснюється керівником виробничої практики від кафедри та підприємства.

За оформлення звіту та щоденника студент отримує 20 балів.

За виконання завдань практики студент отримує 30 балів.

При захисті звіту з практики за якість презентації практики студент отримує 20 балів. При захисті звіту з практики за чіткі та обґрунтовані відповіді на питання при захисті звіту з виробничої практики здобувач отримує 30 балів.

Сумарна оцінка виставляється за такою системою:

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл.1 «Положення про екзамени та заліки у НУБіП України» (наказ про уведення в дію від 26.04.2023 р. № 10):

Табл. 1. Шкала відповідності національної оцінки

Національна	Рейтинг здобувача вищої освіти, бали
Відмінно	**90-100**
Добре	**74-89**
Задовільно	**60-73**
Незадовільно	**0-59**

8. Методичне забезпечення

Електронний курс «Виробнича практика» на платформі Moodle (https://elearn.nubip.edu.ua/course/view.php?id=5065) вміщує повне методичне забезпечення включаючи: шаблон щоденника виробничої практики, робочої програми виробничої практики, глосарій термінів тощо.

9. Рекомендована література

Базова

1. ДСТУ 3008-95 Документація. Звіти у сфері науки і техніки. Структура і правила оформлення.

Допоміжна

1. Николайчук Я.М., Возна Н.Я., Пітух І.Р. Проектування спеціалізованих комп'ютерних систем / Навчальний посібник / - Тернопіль: ТзОВ "Терно граф". 2010. – 392 с., іл.

2. 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..

15. Інформаційні ресурси

https://elearn.nubip.edu.ua/course/view.php?id=5065

16. Нормативна література

1. ДСТУ 2396-94 Системи оброблення інформації. Теорія інформації. Терміни та визначення

2. ДСТУ 2481-94 Системи оброблення інформації. Інтелектуальні інформаційні технології. Терміни та визначення

3. ДСТУ 2482-94 Системи оброблення інформації. Комп'ютерні технології навчання. Терміни та визначення

4. ДСТУ/ISO/IEC 2382-32-2003 Інформаційні технології. Словник термінів. Частина 32. Електронна пошта (ISO 2382-32-2003)

5. Закон України «Про інформацію» від 02.10.1992 № 2657-XII

6. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР

7. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373

8. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

9. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96

10. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі

11. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу

12. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

13. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2

14. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу

15. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі

16. 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

17. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.