

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ІМЕНІ ВАСИЛЯ СТУСА

ФІЗИКО-ТЕХНІЧНИЙ ФАКУЛЬТЕТ  
КАФЕДРА РАДІОФІЗИКИ ТА КІБЕРБЕЗПЕКИ

**ЗАТВЕРДЖЕНО**

на засіданні вченої ради фізико-технічного  
факультету протокол № 4 від 24.09.2019 р.

Голова ради Барибін О.І.



**РОБОЧА ПРОГРАМА**

**З ОЗНАЙОМЧОЇ НАВЧАЛЬНОЇ ПРАКТИЧНОЇ ПІДГОТОВКИ**

ступінь освіти

Бакалавр

(бакалавр, магістр)

галузь знань

12 Інформаційні технології

(шифр і назва)

спеціальність

125 Кібербезпека

(шифр і назва)

освітня програма

Кібербезпека

(шифр і назва)

Вінниця - 2019

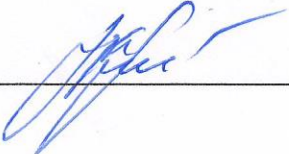
**ЛИСТ ПОГОДЖЕННЯ  
РОБОЧОЇ ПРОГРАМИ ПРАКТИЧНОЇ ПІДГОТОВКИ**

**РЕКОМЕНДОВАНО**

Навчально-методичною комісією фізико-технічного факультету  
протокол № 1 від 20.09 2019 р.

Голова 

**Керівник проектної групи (гарант освітньої програми):**

 Крижановський В.Г.

**ІНІЦІЙОВАНО:**

Кафедрою радіофізики та кібербезпеки  
протокол № 1 від 27.08 2019 р.

Завідувач кафедри

 Барибін О.І.

## ВСТУП

Робоча програма навчальної (ознайомчої) практики складена відповідно до навчального плану підготовки здобувачів вищої освіти СО «Бакалавр» спеціальності 125 Кібербезпека освітньої програми «Кібербезпека».

*Метою практики є формування базових знань та вмінь здобувача вищої освіти із загальних питань інформаційних технологій та інформаційної безпеки.*

**Проходження навчальної (ознайомчої) практики передбачає формування та розвиток у здобувачів вищої освіти компетентностей (як загальних, так і фахових) та програмних результатів навчання відповідно до освітньої програми «Кібербезпека» спеціальності 125 Кібербезпека.**

### *Загальні компетентності (ЗК):*

ЗК-1 Здатність застосовувати знання у практичних ситуаціях.

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-4 Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

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 та/або кібербезпекою.

ФК-11 Здатність виконувати моніторинг ресурсів і процесів функціонування, 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 встановленої політики інформаційної та/або кібербезпеки.

***Програмні результати навчання (ПРН):***

ПРН-1 Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

ПРН-2 Організувати 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 частотої 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-54 Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

## 1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	Опис підготовки фахівців	Характеристика навчальної дисципліни
		денна форма навчання
Кількість кредитів – 3	Галузь знань <b>12 Інформаційні технології</b>	Професійної та практичної підготовки
Модулів – не передбачено	Спеціальність: <b>125 Кібербезпека</b> Освітня програма <b>Кібербезпека</b>	<b>Рік підготовки:</b>
Змістових модулів – не передбачено		1-й
Загальна кількість годин – 90		<b>Семестр</b>
		2-й
Тижневих годин для денної форми навчання: самостійної роботи здобувача – 45	Рівень вищої освіти: <b>Перший</b> Ступінь вищої освіти: <b>бакалавр</b>	не передбачено
		<b>Практичні, семінарські</b>
		не передбачено
		<b>Лабораторні</b>
		не передбачено
		<b>Самостійна робота</b>
		90 год.
		<b>Вид контролю:</b>
диференційований залік		

## **2. ОСНОВНІ ЗАВДАННЯ НАВЧАЛЬНОЇ (ОЗНАЙОМЧОЇ) ПРАКТИКИ**

Основними завданнями є

- набуття навичок самостійного опрацювання теоретичного матеріалу;
- набуття навичок самостійності у роботі;
- набуття навичок роботи у команді, відповідальності за якість та достовірність результатів;
- набуття визначених освітньою програмою компетентностей та програмних результатів навчання;
- набуття практичних навичок відповідно до індивідуального завдання.

## **3. БАЗА ПРАКТИКИ**

Практика проходить на базі навчальних лабораторій кафедри радіофізики та кібербезпеки Донецького національного університету імені Василя Стуса.

База практики задовольняє таким вимогам:

- має висококваліфікований склад викладачів;
- має достатню матеріальну базу для проведення практики.

## **4. ОРГАНІЗАЦІЯ НАВЧАЛЬНОЇ (ОЗНАЙОМЧОЇ) ПРАКТИКИ**

Навчальна практика проводиться у 2 семестрі протягом 2 тижнів. Перед початком практики проводиться настановча конференція, на якій керівники практики від кафедри та факультету ознайомлюють здобувачів вищої освіти ознайомлюють зі змістом, завданнями та організацією практики, веденням документації, правилами формування звіту та критеріями оцінювання.

Відповідальність за організацію, проведення і контроль практики здобувачів вищої освіти з спеціальності 125 «Кібербезпека» ОП

«Кібербезпека» покладається на завідувача кафедрою.

Для безпосереднього керівництва навчальною практикою, кафедрою призначаються керівники з числа штатних працівників. Керівництво практикою включається до навчального навантаження викладачів.

## **5. КЕРІВНИЦТВО НАВЧАЛЬНОЮ (ОЗНАЙОМЧОЮ) ПРАКТИКОЮ**

Керівництво навчальною практикою здійснюється викладачами кафедри радіофізики та кібербезпеки.

Протягом практики керівники практики:

- проводять інструктажі та консультують здобувачів вищої освіти щодо формування та виконання індивідуального завдання;
- здійснюють контроль за роботою здобувачів вищої освіти під час практики та за необхідності вносять корективи по виконанню календарного-плану графіку;
- надають відгук про проходження навчальної (ознайомчої) практики здобувачам вищої освіти, якими вони керували;
- звітують перед кафедрою про хід та підсумки навчальної (ознайомчої) практики.

## **6. ЗМІСТОВНІ МОДУЛІ**

Зміст навчальної (ознайомчої) практики повинен охоплювати такі напрями навчального та виховного процесу: навчально-методичну, виховну та індивідуальну роботу.

### ***Навчально-методична робота***

- ознайомлення із теоретичними основами технологій, що використовуються в рамках індивідуального завдання;
- засвоєння сучасних методів навчання.



### ***Виховна робота***

- набуття навичок роботи у команді;
- набуття навичок самостійного ведення роботи.

### ***Індивідуальна робота***

- виконання практичної частини відповідно до індивідуального завдання.

## **7. КАЛЕНДАРНИЙ ПЛАН ПРАКТИКИ**

Робочі дні по порядку	Тема заняття, основний зміст роботи
1	Вступне заняття «Організація практики та техніка безпеки». Розподіл здобувачів за безпосередніми керівниками. Вивчення здобувачем програми практики. Отримання індивідуальних завдань.
2-10	Виконання здобувачем індивідуального завдання, виданого керівником.
11-14	Формування та оформлення звіту.

## **8. ОРГАНІЗАЦІЙНІ ВИМОГИ**

1. Здобувач повинен щодня працювати над виконанням індивідуального завдання **не менше 6 годин**.

2. Двічі на тиждень здобувач повинен звітувати перед керівником практики про виконання календарного плану.

3. Кожний здобувач повинен виконати індивідуальне завдання.

### *Обов'язки здобувачів вищої освіти*

1. У період практики здобувач зобов'язаний дотримуватися правил внутрішнього розпорядку Університету, виконувати завдання керівника практики.

2. Здобувачі зобов'язані виконувати всі види робіт, передбачені

програмою навчальної (ознайомчої) практики.

## 9. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Напрями індивідуальних завдань:

- використання сучасних пакетів прикладних програм, зокрема текстових редакторів та табличних процесорів;
- робота із комп'ютерним апаратним та програмним забезпеченням, вивчення якого передбачено змістом освітньої програми.

Примірні теми індивідуальних завдань:

- діагностика та налаштування апаратного та програмного забезпечення в лабораторіях кафедри,
- налаштування та використання віртуальних машин,
- налаштування параметрів безпеки ОС Windows,
- налаштування параметрів безпеки документу Microsoft Word,
- налаштування параметрів безпеки документу Microsoft Excel,
- налаштування параметрів безпеки документу Microsoft Power Point,
- налаштування параметрів безпеки документу Adobe Acrobat Reader,
- налаштування параметрів безпеки мережевих пристроїв (маршрутизатор, комутатор, тощо),
- використання базових типів даних на різних мовах програмування.

## **10. ПОТОЧНИЙ І ПІДСУМКОВИЙ КОНТРОЛЬ ТА ОЦІНКА РЕЗУЛЬТАТІВ**

Контроль за проходженням навчальної практики здійснюють керівники практики, завідувач кафедри та представники деканату.

Підсумки навчальної (ознайомчої) практики узагальнюються на засіданні кафедри.

Здобувач вищої освіти подає на кафедру звіт про практику у вигляді короткої анотації з його індивідуального завдання, заповнений щоденник практики. Без заповненого щоденника практика не зараховується.

Результати навчальної (ознайомчої) практики оцінюються відповідно Порядку оцінювання знань здобувачів вищої освіти у Донецькому національному університеті імені Василя Стуса та враховується при призначенні академічної стипендії на рівні з іншими дисциплінами навчального плану.

## **11. ПЕРЕЛІК І ВИМОГИ ДО ЗВІТНОЇ ДОКУМЕНТАЦІЇ**

Наприкінці навчальної (ознайомчої) практики здобувач зобов'язаний надати керівникові практики наступну документацію:

1. Щоденник проходження навчальної практики.
2. Звіт з виконання індивідуального завдання.

### **Вимоги до звіту**

Звіт повинен бути виконаний у друкованому вигляді на аркушах білого паперу формату А4 (210×297 мм) з використанням текстового редактора Word відповідно до таких вимог:

- шрифт – Times New Roman (для значенневого виділення прикладів, понять тощо допускається використання інших шрифтів);
- кегль – 14 пт;
- міжрядковий інтервал – 1,5 (до 30 рядків на сторінці);
- верхні та нижні поля – 20 мм, ліве – 30 мм, праве – не менше 10 мм.

Звіт повинен мати титульний аркуш з позначенням назви університету, кафедри, групи, прізвища здобувача вищої освіти, а також посади і прізвища керівника практики.

Заголовок розділу, підрозділу від попереднього тексту відокремлюють трьома інтервалами. Відступ від назви підрозділу (пункту, підпункту) до наступного тексту повинен складати півтора інтервала. Назви розділів та підрозділів для зручності читання потрібно виділяти напівжирним шрифтом, а визначення понять у тексті та термінів – курсивом.

Загальний обсяг звіту повинен становити до 20 сторінок друкованого тексту.

У звіті повинно бути відображено наступні позиції:

- опис індивідуального завдання;
- теоретичні відомості про область, що вивчається;
- опис виконання індивідуального завдання;
- досягненні результати;
- список використаної літератури.

## **РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1. ДСТУ 3008-95. Документація. Звіти у сфері науки і техніки [Текст]: структура і правила оформлення. - Введ.01.01.1996. - Київ: Держстандарт України, 1995. - 37 стор.

2. ДСТУ ГОСТ 7.1:2006. Бібліографічний запис. Бібліографічний опис [Текст]: загальні вимоги та правила складання. - Введ.01.07.2007. - Київ: Держстандарт України, 2007. - 64 стор.

3. Bucki L.A. Microsoft Word 2013 Bible. - John Wiley & Sons, Inc., 2013. -1010 p. Англ. мовою.

4. Lambert J. MOS 2016 Study Guide for Microsoft Excel. - Microsoft

Press, 2016.-192 p.

5. В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. «Інформаційна та кібербезпека: соціотехнічний аспект». - 2015.

6. Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security // International Technical Support Organization. – Dec. 2010.

7. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва онографія. – К. : НІСД, 2014. – 328 с. — ISBN 978-966-554-240-7

8. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник Київ: ООО Д.В.К., 2004. - 508 с. За ред. Кривуци В. Г. ISBN 966-6313-1-0.

9. Матвієнко М.П., Розен В.П. Комп'ютерна схемотехніка. Навчальний посібник. – К.: Ліра-К, 2015. – 192 с.

10. Замула О.А., Горбенко Ю.І., Шумов А.І. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації»: Навч. посібник. - Харків: ХНУРЕ, 2010

11. Курко А. М. Введення в теорію інформації //Посібник до вивчення дисципліни «Теорія інформації» / А. М. Курко, В. Я. Решетняк. Тернопіль: Тернопільський національний технічний університет ім. І. Пулюя. 2017 – 108с.

12. Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П. Комп'ютерні мережі: навчальний посібник. — Вінниця: ВНТУ, 2013. —371 с.

13. Машкаров Ю.Г.Комп'ютерні мережі та телекомунікації Навч. посіб. / Ю. Г. Машкаров, І. В. Кобзев, О. В. Орлов, М. В. Мордвинцев. - Х. : Вид-во Хнавч. посіб. / Ю. Г. Машкаров, І. В. Кобзев, О. В. Орлов, М. В. Мордвинцев. - Х. : Вид-во ХарРІ НАДУ "Магістр", 2012. - 212 с.

14. Рамський Ю.С., Олексюк В.П., Балик А.В. Адміністрування

комп'ютерних мереж і систем Навчальний посібник -Тернопіль: Навчальна книга – Богдан, 2010. -201стор.