МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ

Факультет інформаційних технологій та кібербезпеки
Кафедра кібербезпеки та технічного захисту інформації

НАСКРІЗНА ПРОГРАМА ПРАКТИКИ

Освітня (професійна, наукова) програма	Кібербезпека та захист інформації
Спеціальність	125 Кібербезпека та захист інформації
Галузь знань	12 Інформаційні технології
Рівень вищої освіти	Перший (бакалаврський)

ОДЕСА – 2024

Наскрізна програма практики за ОПП «Кібербезпека та захист інформації» для здобувачів першого (бакалаврського) рівня вищої освіти зі спеціальності 125 Кібербезпека та захист інформації / Уклад.: І.В. Лімарь, Ю.В. Бєлова. Одеса : ДУІТЗ (Електр. вид. https://metod.suitt.edu.ua), 2024. 19 с.

Укладачі:

Лімарь Ігор Валерійович, к.т.н., старший викладач кафедри кібербезпеки та технічного захисту інформації;

Бєлова Юлія Володимирівна, викладач кафедри кібербезпеки та технічного захисту інформації.

Наскрізна програма практики за освітньо-професійною програмою «Кібербезпека та захист інформації» для здобувачів першого (бакалаврського) рівня вищої освіти зі спеціальності 125 Кібербезпека та захист інформації розглянута засіданні кафедри Кібербезпеки та технічного захисту інформації (протокол від «28» травня 2024 р. № 9).

Завідувач кафедри _____ Володимир КОРЧИНСЬКИЙ

Погоджено з гарантом освітньо-професійної програми

_____ Олексій ОНАЦЬКИЙ

Ухвалено рішенням Навчально-методичної ради Державного університету інтелектуальних технологій і зв'язку (протокол від «28» червня 2024 р. № 8).

Голова навчально-методичної ради

_____ Світлана ХАДЖИРАДЄВА

ВСТУП

Практика здобувачів вищої освіти Державного університету інтелектуальних технологій і зв'язку є невід'ємною складовою освітньо-професійних і освітньо-наукових програм підготовки здобувачів вищої освіти. Вона спрямована на формування загальних і фахових компетентностей здобувачів вищої освіти, закріплення теоретичних знань, отриманих за час навчання, набуття і удосконалення практичних умінь та навичок за відповідною спеціальністю.

Основними принципами організації практики є: систематичність, наступність, ускладнення її змісту й методів у порівнянні з попередніми видами; комплексність, яка забезпечує міжпредметні зв'язки навчальних дисциплін (компонентів) професійної та практичної підготовки, що вивчаються в Університеті; диференціація та індивідуалізація змісту та форм організації практики.

Практика здобувачів вищої освіти виконує такі функції: діагностичну (визначає ступінь готовності до майбутньої професійної діяльності); освітню (удосконалює набуту професійну компетентність); корекційну (уточнює окремі параметри набутої професійної компетентності, підвищує дієвість знань, удосконалює професійні уміння, сприяючи професійній ідентифікації); конструктивно-організаторську (включає в реальний процес реалізації професійної компетентності); комунікативну.

1. МЕТА ТА ЗАВДАННЯ ПРАКТИЧНОЇ ПІДГОТОВКИ ЗДОБУВАЧІВ

Мета практики: формування та розвиток у здобувачів першого (бакалаврський) рівня вищої освіти практичних умінь та навичок щодо вирішення практичних завдань, а також набуття й удосконалення компетентностей, визначених освітньо-професійною програмою спеціальності 125 Кібербезпека та захист інформації, ґрунтуючись на базових теоретичних положеннях, сучасних концепціях, моделях, принципах, практичних рекомендаціях тощо.

2. ВИДИ ТА ОПИС ПРАКТИК

Відповідно до навчального плану підготовки здобувачів першого (бакалаврський) рівня вищої освіти за освітньо-професійною програмою «Кібербезпека та захист інформації» зі спеціальності 125 Кібербезпека та захист інформації передбачено два види практик (табл. 1).

Таблиця 1

Види, назва і тривалість практики здобувачів вищої освіти за освітньо-професійною програмою «Кібербезпека та захист інформації» зі спеціальності 125 Кібербезпека та захист інформації

№ п/п	Назва практики	Семестр	Кількість кредитів ЄКТС
1	Виробнича практика	6	4 (120)
2	Переддипломна практика	8	3 (90)

2.1. Виробнича практика

Мета виробничої практики – поглиблення знань у виробничих умовах і застосування теоретичних знань, отриманих студентами у процесі навчання, та здобуття ними навиків самостійної практичної діяльності з напрямку своєї майбутньої професії; оволодіння сучасними методами, формами організації праці в галузі майбутньої професії; набуття професійних умінь і навичок, необхідних для прийняття самостійних рішень; надбання практичного досвіду, розвиток професійного мислення, закріплення навичок організаторської та комерційної діяльності у трудовому колективі; систематичне поновлення знань студентами; формування професійної компетентності.

Провідне завдання виробничої практики згідно з її метою є:
закріплення отриманих в ДУІТЗ знань з фахових дисциплін спеціальності 125 Кібербезпека та захист інформації;

– набуття та вдосконалення студентами практичних навичок у розв’язанні конкретних питань, пов’язаних з організацією захисту інформації на підприємстві, методології виконання проектів та оформленням технічної документації;

– ознайомлення з роботою підприємств, організацій різних форм власності та установ, із досвідом організації інформаційних технологій на підприємстві;

– самостійне виконання студентами індивідуальних або групових завдань керівника практики від бази практики;

– вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації на підприємстві;

– навчитись застосовувати теорії та методи захисту для забезпечення безпеки інформації на підприємстві;

– оволодіння навичками організаційно-управлінської роботи;

– складання звіту про виконання програми практики.

Очікувані програмні результати навчання:

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 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 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

Унаслідок досягнення результатів практичної підготовки здобувачі вищої освіти в контексті змісту різних видів практики мають опанувати такі компетентності:

***загальні компетентності*:**

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професії.

ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК5. Здатність до пошуку, оброблення та аналізу інформації.

ЗК7. 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.

***спеціальні компетентності*:**

СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей 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.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації 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.

СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

СК9. Здатність здійснювати професійну діяльність на основі впровадження системи управління інформаційною та/або кібербезпекою.

СК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

СК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Зміст виробничої практики

№ п/п	Зміст практики
1	Проходження інструктажу з техніки безпеки.
2	Ознайомлення з профілем роботи підприємства (галузь, види діяльності), вивчення составу та структури підприємства (відділу) та опис
3	Знайомство з конкретними умовами і змістом роботи персоналу та посадовими обов’язками співробітників у галузі інформаційних технологій.
4	Аналіз та опис наявного інформаційного, організаційного, програмного, апаратного та інших забезпечень, що застосовуються на базі практики
5	Виконання обов’язків згідно посади практики на підприємстві (організації, установі, компанії). Виконання програми виробничої практики за індивідуальним планом
6	Узагальнення результатів роботи. Ведення щоденника практики.
7	Дослідження літературних або інших джерел наукового та практичного спрямування, які стосуються вирішення задач практики
8	Оформлення щоденника, звіту з практики та презентації.

Форма та метод контролю:
форма: екзамен
метод: заключна конференція / захист звіту

Порядок оформлення та ведення щоденника з практики:
У щоденнику відображені набуті практичні навички здобувача.

Щоденник містить інформацію щодо виконаної роботи щоденно відповідно до завдань виробничої практики, а саме:

– **календарний графік проходження практики:** складання та оформлення календарного графіку проходження практики за назвами робіт, тижнями проходження практики та відмітками про виконання.

– **робочі записи під час практики** за датами та змістом робочих записів.

– **індивідуальне завдання.** Формування та оформлення індивідуальних завдань (можливі варіанти):

– аналіз об'єкту захисту. Аналіз рівня комп'ютерного забезпечення об'єкту. Аналіз периферійного та мережевого обладнання, локальної комп'ютерної мережі бази практики та ін. Технічна, нормативна документація

– аналіз і оцінка ризиків інформаційної безпеки. Аналіз вразливостей комп'ютерних систем та мереж. Оцінка вразливостей в комп'ютерних системах та мережах.

– організація комплексної безпеки об'єктів. Структура та рівні мережевої взаємодії при побудові КСБ. Програмно-апаратні рішення в комплексних систем безпеки.

2.2. Переддипломна практика

Мета та завдання практики (переддипломної) – Метою переддипломної практики для студентів спеціальності 125 «Кібербезпека та захист інформації» є завершення формування у випускника професійних практичних навичок, необхідних для роботи на підприємствах, застосування отриманих професійних знань, поглиблення та закріплення теоретичних положень з фахових дисциплін, завершення формування бази фактичних знань для виконання кваліфікаційної роботи та практичного використання знань в галузі інформаційних технологій для ефективного розв'язування складних спеціалізованих завдань та практичних проблем під час професійної діяльності у сфері кібербезпеки.

До цілей переддипломної практики слід віднести:

– забезпечення єдності теоретичного і практичного навчання студентів з питань організації діяльності підрозділів, відділів, структур та окремих фахівців із захисту інформації, включаючи особливості функціонування підприємств та вирішуваних ними завдань;

– поглиблення і закріплення теоретичних знань з фахових дисциплін;

– застосування отриманих у процесі навчання знань безпосередньо в межах організаційної структури, де проходить практика (бази переддипломної практики);

– формування прикладних професійних навичок, необхідних для здійснення майбутньої професійної діяльності;

– доповнення знань за окремими питаннями, пов’язаними з темою дипломної роботи, збір та обробка даних, необхідних для її написання;

– набуття навичок самостійної роботи за спеціальністю;

– перетворення фундаментальних і прикладних знань за фахом у професійні функції, формування досвіду професійної діяльності, професійно і соціально значущих якостей особистості сучасного фахівця із акцентом на розвиток творчого потенціалу, самостійності та ініціативності, уміння приймати рішення в реальних умовах, здатності працювати в команді;

– опанування навичок аналізу, інтерпретації інформації, вироблення конструктивних пропозицій, формування дослідницьких, аналітичних, організаторських, комунікативних якостей;

– отримання навичок проведення аналізу інформаційних систем конкретного об'єкту управління з метою самостійного проєктування та розробки елементів захищених автоматизованих інформаційних систем з використанням сучасних інформаційних технологій та розвинутих інструментальних засобів захисту інформації;

– опанування навичок командної роботи, а також самостійного прийняття рішень, дотримання норм і правил професійної етики.

Програма і завдання переддипломної практики орієнтовані на виконання основного її завдання – набуття студентами компетентностей та досягнення результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності «Кібербезпека».

Завдання практики:

– навчити студентів використовувати в реальних умовах підприємства (установи, організації, закладу, фірми тощо – далі під загальним терміном «підприємство») отримані теоретичні і практичні знання зі спеціальності;

– формування у студентів практичних навичок в роботі з програмним та програмно-апаратним забезпеченням, комп’ютерними системами та мережами, базами даних та знань на підприємстві в аспекті забезпечення їх інформаційної та/або кібербезпеки;

– оволодіння сучасними методами, формами організації роботи за спеціальністю (практичними навичками з організації і автоматизації захисту інформації, інформаційних систем та процесів, безпечного функціонування автоматизованих інформаційних систем і мереж тощо);

– засвоєння на практиці структури інформаційно-аналітичної діяльності та загальнонаукових і спеціальних методів, що застосовуються в управлінні захистом інформації;

– розвити у студентів професійне вміння приймати самостійні рішення під час виконання фахових завдань і підготовки звітів з виконаної роботи.

Під час проходження практики студенти повинні ознайомитися на базі практики (за узгодженням з керівником практики від підприємства) з існуючими

інформаційними, інформаційно-телекомунікаційними, комп'ютеризованими системами та засобами автоматизації, спеціалізованими і комплексними системами захисту інформації, та виконати наступні завдання:

– отримати практичні знання та навички за фахом на підприємствах;

– закріпити знання отриманих під час навчання у ЗВО;

- вивчити і проаналізувати діяльність даного підприємства, дослідити об'єкт практики, структуру та функції підрозділів об'єкта практики, їх взаємозв'язок і взаємодію;

– провести аналіз предметної області та виявити наявні проблем в сфері захисту інформації;

– підібрати і вивчити первинні матеріали за темою роботи;

– провести порівняльний аналіз переваг і недоліків існуючих рішень;

– ознайомитися із заходами щодо підвищення кібербезпеки та інформаційної безпеки, автоматизації бізнес-процесів і реінжинірингу бізнес-систем;

– закріпити та розширити знання з методичного, програмного, технічного, інформаційного та організаційного забезпечення засобами захисту інформації;

– вивчити і проаналізувати актуальні питання проєктування та захисту інформаційних систем для різних сфер внутрішньої та бізнес-діяльності підприємства;

– сформувати рекомендації щодо поліпшення інформаційної безпеки підприємства, оптимізації комп'ютерних ресурсів, тестування та верифікації апаратного і програмного забезпечення;

– запропонувати власні пропозиції щодо організації і вдосконалення інформаційно-телекомунікаційних систем та механізмів (засобів) їх захисту, нові мережні рішення і технології їх впровадження та експлуатації тощо;

– виконати поставлене індивідуальне завдання та оформити звіт з проходження практики;

– розробити технічне завдання на розробку інформаційно-комунікаційної системи в цілому і її окремих складових, а також елементів її захисту в цілому і окремих її ресурсів і складових для виконання кваліфікаційної роботи.

Для успішного виконання завдань переддипломної практики студенту необхідно чітко дотримуватися рекомендованого календарного графіка проходження практики.

З боку бази практики для успішного виконання завдань переддипломної практики студенту мають бути створені сприятливі умови, що забезпечують не тільки закріплення студентами теоретичних знань зі спеціальних предметів, але й набуття ними практичних навичок роботи за спеціальністю на основі глибокого вивчення досвіду забезпечення безпеки мережевих ресурсів та криптографічного захисту інформації в системах інформаційної та/або кібербезпеки; забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації на системах різних рівнів.

В результаті проходження практики, студент має практично оволодіти

передбаченими програмою практики засобами проєктування процесів і систем захисту інформації та підготовки звітної документації, ознайомитись з універсальним і спеціалізованим обладнанням та програмним забезпеченням, що використовується на підприємстві. В ході її проходження передбачено поточний контроль, а в підсумку – захист звіту і залік за результатами захисту.

Очікувані програмні результати навчання:

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 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 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки.

ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

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 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.

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-

телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та кібербезпеки відповідно до цілей і завдань організації.

ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

Унаслідок досягнення результатів практичної підготовки здобувачі вищої освіти в контексті змісту різних видів практики мають опанувати такі компетентності:

***загальні компетентності*:**

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК5. Здатність до пошуку, оброблення та аналізу інформації.

ЗК7. 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.

***спеціальні 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.

СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей 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.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації 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.).

СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

СК9. Здатність здійснювати професійну діяльність на основі впровадження системи управління інформаційною та/або кібербезпекою.

СК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

СК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки

Зміст переддипломної практики

№ п/п	Зміст практики
1	Інструктаж з техніки безпеки. Ознайомлення та вивчення інструкцій та правил техніки безпеки на об’єкті. Вивчення інструкцій пожежної безпеки. Складання іспиту з техніки безпеки та пожежної безпеки.
2	Знайомство із структурою організації. Ознайомлення з поняттям організаційно-штатної структури підприємства. Вивчення призначенням і структури власне організації: розміщення, склад, взаємозв’язки, правила внутрішнього розпорядку,

	організація роботи обслуговуючого персоналу.
3	Організація робіт із захисту інформації на об'єкті інформаційної діяльності (ОІД). Дослідження об'єкту інформаційної діяльності. Ознайомлення та вибір порядку та методики проведення дослідження ОІД. Вивчення нормативно-технічної документації, планів приміщення. Виконання дослідження інформаційного, фізичного, технологічного середовища та середовища користувачів. Розробка моделей загроз та порушника: визначення видів загроз, їх класифікації, істотних загроз (витік інформації технічними каналами та каналами спеціального впливу), методів та способів їх здійснення, класифікації порушника при складанні моделі порушника. Розробка політики безпеки і організація охорони ОІД, пропускного режиму та контролю відвідувачів. Складання плану служби безпеки ОІД, загальної концепції безпеки інформації та контролю доступу.
4	Організаційні заходи захисту інформації на ОІД. Розбиття ОІД на зони безпеки. Ознайомлення та вивчення правил розбиття ОІД на зони безпеки. Створення рубежів безпеки, типових зон безпеки. Розробка організаційних заходів при роботі із співробітниками, організації діловодства та електронного документообігу: управління персоналом підприємства з урахуванням питань захисту інформації з обмеженим доступом, які необхідно здійснювати під час проведення процесу діловодства та електронного документообігу.

Форма та метод контролю:
форма: екзамен
метод: заключна конференція / захист звіту.

Порядок оформлення та ведення щоденника з практики:

У щоденнику відображені набуті практичні навички здобувача.

Щоденник містить інформацію щодо виконаної роботи щоденно відповідно до завдань переддипломної практики, а саме:

– **календарний графік проходження практики:** складання та оформлення календарного графіку проходження практики за назвами робіт, тижнями проходження практики та відмітками про виконання.

– **робочі записи під час практики** за датами та змістом робочих записів.

– **індивідуальне завдання.** Крім загальних завдань, кожен студент обов'язково має виконати індивідуальне завдання з практики і написати звіт з неї. Індивідуальне завдання є однією з форм набуття фахових компетентностей, яке має на меті поглиблення, узагальнення та закріплення знань, які студенти отримали у процесі теоретичного навчання, та застосування цих знань в практичній діяльності. Напрями і тематика індивідуальних завдань для студентів-практикантів розробляються на випусковій кафедрі, виходячи з теми і завдань дипломної роботи, схильностей, здібностей, особливостей студентів та їх уподобань.

Індивідуальне завдання є особистим для кожного студента, визначається керівником практики спільно з керівником кваліфікаційної роботи та виконується у відповідності до її тематики. Індивідуальні завдання виконують студенти самостійно у супроводженні керівника практики. Як правило, індивідуальні завдання виконуються окремо кожним студентом. У тих випадках, коли завдання

мають комплексний характер, до їх виконання можуть залучатися кілька студентів.

Тематика індивідуальних завдань повинна відповідати кваліфікаційній характеристиці бакалавра спеціальності. Тему завдання вибирають з урахуванням сфери інтересів студента, специфіки дослідно-конструкторської або науково-дослідної роботи керівника практики від кафедри та специфіки роботи підприємства – бази практики. Тема завдання може бути обрана студентом самостійно і прийнята до виконання за умови її погодження з керівниками від кафедри та підприємства.

Приклади індивідуальних завдань переддипломної практики (завдання складаються і уточнюються з урахуванням специфіки діяльності і можливостей бази практики):

1 Дослідження технології контролю оперативного стану інформаційної системи.

2 Дослідження механізмів впливу відмов апаратного забезпечення на стабільність роботи дата-центрів.

3 Дослідження системи управління персоналом з питань інформаційної безпеки підприємства.

4 Організація захисту користувацького контенту від копіювання на вебресурсі.

5 Дослідження технологій ідентифікації та аутентифікації користувачів в інформаційно-комунікаційних системах та мережах.

6 Дослідження механізмів інформаційної безпеки при розгортанні систем широкосмугового зв’язку Wi-Fi.

7 Дослідження технологій забезпечення безпеки соціотехнічних систем від складних інформаційних атак.

8 Дослідження технічних системи контролю та управління доступом до приміщень.

9 Дослідження технологій захисту інформації на віртуальних цифрових носіях.

10 Дослідження технологій забезпечення безпеки документів в системах електронного документообігу.

11 Дослідження захисту інформаційних каналів управління автоматизованою системою супутникового зв'язку.

12 Дослідження технологій вибору проєктної альтернативи системи захисту інформації корпоративної інформаційно-аналітичної системи.

13 Дослідження технологій забезпечення безпеки віртуальних спільнот в інтернет середовищі соціальних мереж.

14 Дослідження технологій управління інцидентами інформаційної безпеки з використанням можливостей DLP-систем.

15 Дослідження політик безпеки і систем контролю доступу для локальних обчислювальних мереж.

16 Дослідження алгоритмів та програмного забезпечення маскування даних.

17 Дослідження засобів захисту пристроїв в IoT.

18 Дослідження технологій створення системи протидії впливу злоякісного

коду, шпигунського і завідомо фальшивого програмного забезпечення.

19 Дослідження процесу створення захищеної корпоративної мережі з застосуванням технологій VPN.

20 Дослідження засобів захисту інформації системи «розумний дім».

Виконанню індивідуальних завдань необхідно приділяти значну увагу для розвитку самостійності у студентів при вирішенні технічних питань та розширення їх кругозору як невід'ємної складової розвитку навичок. Серед загальних технологій навчання, орієнтованих на розвиток навичок, до застосування під час проходження переддипломної практики слід рекомендувати:

- застосування рольових технологій при виконанні завдань практики з визначенням (за можливістю, зі зміною посадових обов'язків) студента-практиканта на робочому місці (декількох робочих місцях) при виконанні фахових завдань у реальних умовах діяльності підприємства, що сприяє розвитку навичок адаптованості, прояву ініціативи та засвоєння нового досвіду, роботи в команді, ділової етики, дружності і вміння володіти собою;

- регламентування часу на виконання завдань практики, чітке визначення термінів проходження контрольних точок сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту);

- спілкування з керівниками практики, різними посадовими особами, прилюдні виступи під час захисту звітів з обґрунтуванням прийнятих рішень щодо вибору методів розв'язування задач в діалозі з викладачем і групою – такі методи сприяють формуванню і удосконаленню вмінь публічних виступів, спілкування, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики тощо.

2.3. Перелік рекомендованих баз практик для бакалаврів факультету Інформаційних технологій та кібербезпеки, що навчаються за спеціальністю 125 – Кібербезпека та захист інформації

№	Назва компанії	№ договору	Напрям роботи компанії
1	Міжнародна академія менеджменту безпеки	17-08/23 від 17.09.2023	Освітні послуги
2	Освітній фонд "Кіпсолид"	б/н від 29.03.2023	Освітні послуги
3	ТОВ "Робер Бош ЛТД"	ВТ-20230317 від 17.03.2023	Вендор та інсталятор систем безпеки
4	ПП "Ардо"	б/н	Проектування, монтаж та обслуговування систем безпеки
5	ТОВ Багатопрофільна фірма "СекретСервіс"	01/12-ПД від 07.12.2023	Проектування, монтаж та обслуговування систем безпеки
6	ТОВ "Ю-Контрол"	б/н від 17.10.2022	Перевірка контрагентів, конкурентна розвідка
7	ТОВ "ТІРАС-12"	01-17/180 від 21.06.2022	Виробництво систем безпеки
8	ТОВ "Консалтинговна компанія "СІДКОН"	28-01/22 від 28.01.2022	Консалтингові послуги, аудит безпеки, конкурентна розвідка
9	Департамент кіберполіції	б/н від	Кібербезпека

	Національної поліції України	28.06.2023	
10	ТОВ “ГОФЕР КОРПОРЕЙШН”	01/02-ПД від 08.02.2022	Розробка систем безпеки
11	ПП “ЛОДЖІКФОКС”	31/12/22 від 31.12.2022	Виробництво, продаж та інсталяція систем безпеки

3. ЗАГАЛЬНІ ВИМОГИ ДО ЗВІТІВ ТА ПІДВЕДЕННЯ ПІДСУМКІВ ПРАКТИКИ

Після закінчення терміну практики здобувачі звітують про виконання програми та індивідуального завдання. Форма звітності здобувача за практику – це подання звіту, підписаного і оціненого безпосередньо керівником від бази практики в друкованому вигляді. Звіт разом з іншими документами, встановленими навчальним закладом (щоденник, характеристика та ін.), подається на рецензування керівнику практики від навчального закладу. Після доопрацювання та остаточного погодження з керівником практики звіт в друкованому вигляді подається на захист. Звіт має містити відомості про виконання студентом усіх розділів програми практики та індивідуального завдання, висновки і пропозиції, список використаної літератури тощо. Текст звіту може містити відповідні розрахунки, пояснення, таблиці, схеми, діаграми тощо. Оформлюється звіт за вимогами, які встановлюються стандартом для оформлення текстових документів. Звіт захищається студентом у формі заліку у вищому навчальному закладі.

Звіт подається на одному боці аркуша білого паперу формату А4 через півтора міжрядкових інтервали шрифт - TimesNewRoman, розмір - 14. Текст необхідно друкувати залишаючи поля таких розмірів: ліве - не менше 25 мм, праве - не менше 10 мм, верхнє і нижнє - не менше 20 мм. Текст звіту поділяють на розділи, підрозділи і пункти відповідно до структури програми практики. Складений здобувачем звіт має наскрізну нумерацію сторінок.

Звітні документи:

1. **Щоденник до всіх видів практик,** у якому відображена особистісна і професійна рефлексія діяльності здобувача.
2. **Пакет звітних матеріалів до всіх видів практик: х**арактеристика з місця проходження практики з рекомендованою оцінкою; Звіт

Підведення підсумків практики

Після закінчення терміну практики здобувачі звітують про виконання програми практики у визначені терміни.

Здобувачі у триденний термін після закінчення практики надають керівникові практики письмовий звіт про проходження практики та оформлений за всіма розділами щоденник практики з дотриманням відповідних стандартів щодо оформлення такої документації, підписаний керівником від бази практики. До письмового звіту додаються матеріали, визначені робочою програмою практики

та індивідуальним планом проходження практики здобувачами.

Формою підсумкового контролю з практики є залік. Залік з практики проводить комісія, що призначається завідувачем кафедри. До складу комісії входять керівник практики з фаху, викладачі та (за змогою) керівник від бази практики. Залік проводиться протягом перших десяти робочих днів після закінчення практики, у формі захисту здобувачем звіту з практики.

Оцінка вноситься в заліково-екзаменаційну відомість, у залікову книжку та індивідуальний навчальний план здобувача з підписами членів комісії.

Якщо програма практики не виконана з поважної причини, то здобувач має право пройти практику в наступному навчальному році або за індивідуальним графіком у вільний від навчання час.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	**Шкала ЄКТС**	**Оцінка за національною шкалою**		**Нарахування балів**	**Бали нараховуються таким чином:**
		для іспиту	**для заліку**		
90-100	A	Відмінно	зараховано		***Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою*** і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів, за результати екзамену – до 40 балів. При оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань здобувачів вищої освіти за різними системами
82-89	B	Добре			
74-81	C				
64-73	D	Задовільно			
60-63	E				
35-59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання		
0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	Не зараховано з обов'язковим повторним вивченням дисципліни		

Критерії оцінювання результатів навчання

Оцінка за національною шкалою	**Зміст критеріїв оцінки**
1	*2*
Відмінно (A) – від 90 до 100 балів	Результати студента повністю відповідають завданню практики, матеріал звіту повністю розкриває поставлене завдання. зміст, оформлення звіту й щоденника відповідають стандартам, характеристика студента позитивна. Повні та точні відповіді на всі питання щодо програми практики і виконаної індивідуальної роботи
Дуже добре (B) – від 82 до 89 балів	Отримує студент за повне засвоєння навчального матеріалу, володіння понятійним апаратом, орієнтування в вивченому матеріалі, свідоме використання знань для вирішення практичних завдань, грамотний виклад відповіді, але у змісті і формі відповіді (або звіту) наявні окремі неточності (похибки). У відповідях на запитання членів комісії з програми практики студент загалом має тверді знання.
Добре (C) – від 74 до 81	Є зауваження щодо змісту та оформлення звіту й щоденника. У відповідях на запитання членів комісії з програми практики студент припускається окремих

балів	неточностей, хоча загалом має достатні знання.
Задовільно (D) – від 64 до 73 балів	Недбале оформлення звіту і щоденника. Переважна більшість питань програми практики висвітлена, однак мають місце окремі розрахункові й логічні помилки. Студент виконав практичні завдань, передбачені програмою практики, і за результатами практики виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшої практичної діяльності за професією.
Задовільно (E) – від 60 до 63 балів	Неповне опанування програмного матеріалу, але з відповіді якого слідує, що отримані ним знання і набуті практичні навички відповідають мінімальним критеріям оцінювання.
Незадовільно з можливістю повторного складання (FX) – від 35 до 59 балів	У звіті висвітлені не всі питання, або підготовлена не самостійно. Оформлення роботи є недбалим. Характеристика студента стосовно ставлення до практики і трудової дисципліни негативна. На запитання членів комісії студент не може дати задовільних відповідей
Незадовільно з обов'язковим повторним вивченням дисципліни (F) – від 0 до 34 балів	Виставляється студенту за неявку для проходження переддипломної практики або за зрив її графіка без поважних причин, виявлене під час практики і захисту повне незнання і нерозуміння навчального матеріалу або відмову від захисту.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА:

Основна:

1. Закону України «Про вищу освіту», стаття 51 «Практична підготовка осіб, які навчаються у закладах вищої освіти» (Відомості Верховної Ради, 2014, № 37-38).
2. Положення Про порядок проведення практичної підготовки здобувачів вищої освіти Державного університету інтелектуальних технологій і зв'язку (Затверджено Вченою радою ДУІТЗ протокол №1 від 10.02.2023 р.) polozhennia_pro_poriadok_provedennia_praktychnoi_pidhotovky_zdobuvachiv.pdf (suitt.edu.ua);

Додаткова:

3. Державний стандарт України Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96.
4. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
5. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
6. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.
7. НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.
8. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

9. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
10. НД ТЗІ 2.7-011-12 Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв.
11. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи.
12. НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.
13. 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.
14. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.