

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**

<b>Освітня (професійна, наукова) програма</b>	Кібербезпека та захист інформації
<b>Спеціальність</b>	F5 Кібербезпека та захист інформації
<b>Галузь знань</b>	F Інформаційні технології
<b>Рівень вищої освіти</b>	Перший (бакалаврський)

**Наскрізна програма практики** за ОПП «Кібербезпека та захист інформації» для здобувачів першого (бакалаврського) рівня вищої освіти зі спеціальності F5 Кібербезпека та захист інформації / Уклад.: І.В. Лімарь, Ю.В. Белова. Одеса : ДУІТЗ, 2025. 16 с.

**Укладачі:**

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

Белова Юлія Володимирівна, старший 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 F5 Кібербезпека та захист інформації розглянута засіданні кафедри Кібербезпеки та технічного захисту інформації (протокол від «27» листопада 2025 р. № 5).

Завідувач кафедри



Володимир КОРЧИНСЬКИЙ

Погоджено з гарантом освітньо-професійної програми «Кібербезпека та захист інформації» зі спеціальності F5 Кібербезпека та захист інформації для здобувачів першого (бакалаврського) рівня вищої освіти



Євген ВАСІЛІУ

Наскрізна програма практики освітньо-професійної програми «Кібербезпека та захист інформації» зі спеціальності F5 Кібербезпека та захист інформації ухвалена рішенням Навчально-методичної ради Державного університету інтелектуальних технологій і зв'язку (протокол від «25» грудня 2025 р. № 11).

Голова навчально-методичної ради



Світлана ХАДЖИРАДСВА

## 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, 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 (забезпечує включення практикантів 4 у систему стосунків викладач – академічна група, викладач – здобувач вищої освіти).

## 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 у межах спеціальності F5 Кібербезпека та захист інформації, ґрунтуючись на базових теоретичних положеннях, сучасних концепціях, моделях, принципах, практичних рекомендаціях тощо.

**Завдання практики:** узагальнення, закріплення і поглиблення знань, що отримані під час навчання в університеті для використання їх у подальшій роботі та обґрунтованого прийняття рішень; отримання інформації про ринок затребуваних професій; знайомство з порядком роботи та умовами праці на підприємстві; отримання досвіду входження в трудовий колектив; отримання інформації про те, які знання, отримані в університеті, і в якому напрямі необхідно поглиблювати і розвивати; знайомство з новими технологіями в ІТ-індустрії.

В результаті практичної підготовки здобувачі вищої освіти в контексті змісту різних видів практики мають опанувати такі компетентності:

<b>Загальні компетентності</b>	
ЗК 1	Здатність застосовувати знання у практичних ситуаціях.
ЗК 2	Знання та розуміння предметної області та розуміння професії.
ЗК 5	Здатність вчитися і оволодівати сучасними знаннями
<b>Спеціальні (фахові, предметні) компетентності</b>	
СК1	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.
СК2	Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.
СК7	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
СК9	Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.
<b>Очікувані результати навчання:</b>	
РН 1	Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
РН 4	Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН 5	Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН 6	Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

PH 9	Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
PH 21	Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

## 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 F5 Кібербезпека та захист інформації передбачено два види практик.

**Види, назва і тривалість практики здобувачів вищої освіти за освітньо-професійною програмою «Кібербезпека та захист інформації» зі спеціальності F5 Кібербезпека та захист інформації**

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

### 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 F5 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 проєктів 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.

### Зміст виробничої практики

№ п/п	Зміст практики
1	Проходження інструктажу з техніки безпеки.
2	Ознайомлення з профілем роботи підприємства (галузь, види діяльності), вивчення складу 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 контролю:** екзамен

**Метод контролю:** 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:

1. Календарний графік проходження практики: складання та оформлення календарного графіку проходження практики за назвами робіт, тижнями проходження практики та відмітками про виконання.

2. Робочі записи під час практики за датами та змістом робочих записів.

3. 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.

- Організації 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 F5 «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, професійних 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 проектування 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 та захист інформації».

#### **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;

- розвинути 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 проектування 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 проектування 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.

### **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, пропускнуго 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 контролю:** екзамен

**Метод контролю:** 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:

1. Календарний графік проходження практики: складання та оформлення календарного графіку проходження практики за назвами робіт, тижнями проходження практики та відмітками про виконання.

2. Робочі записи під час практики за датами та змістом робочих записів.

3. 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 користувачького 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 проектної 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 маскуванню даних.

17 Дослідження засобів захисту пристроїв в IoT.

18 Дослідження технологій створення системи протидії впливу зловиясного 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 здобувачів, які навчаються за спеціальністю F5 Кібербезпека та захист інформації

№	Назва компанії	Напрямок роботи компанії
1	2	3
1	Освітній фонд "Кісолід"	Освітні послуги
2	ТОВ "Робер Бош ЛТД"	Вендор та інсталятор систем безпеки
3	ПП "Ардо"	Проектування, монтаж та обслуговування систем безпеки
4	ТОВ Багатопрофільна фірма "Секрет Сервіс"	Проектування, монтаж та обслуговування систем безпеки
5	ТОВ "Ю-Контрол"	Перевірка контрагентів, конкурентна розвідка
6	ТОВ "ТІРАС-12"	Виробництво систем безпеки
7	ТОВ "Консалтингова компанія "СІДКОН"	Консалтингові послуги, аудит безпеки, конкурентна розвідка
8	Департамент кіберполіції Національної поліції України	Державна установа
9	ТОВ "ГОФЕР КОРПОРЕЙШН"	Розробка систем безпеки
10	ПП "ЛОДЖІКФОКС"	Виробництво, продаж та інсталяція систем безпеки
11	ТОВ «КОБІ СС»	Комплексні системи безпеки, інтелектуальні системи відеоспостереження, ІТ (розробка ПЗ)
12	ПП "Південна телекомунікаційна компанія"	Бренд SohoNet. Інтернет-провайдер
13	ІТІ «Біотехніка» НААН	Наука та освіта
14	Головне управління Пенсійного фонду України в Одеській області	Державна установа
15	Одеський обласний центр зайнятості	Державна установа
16	ТОВ «СПО «ЦО – Легіон»	Проектування, монтаж та обслуговування систем безпеки
17	ТОВ «Скайнет Телеком»	Інтернет-провайдер
18	ТОВ «Планета-Юг»	Телекомунікації, кібербезпека, радіотехніка

19	ТОВ «Конкорд-СБ»	Проектування, монтаж систем безпеки
20	Комунальне підприємство «Регіональний офіс міжнародного співробітництва в Одеській області»	Державна установа
21	ТОВ «АНТЕ МЕДІАМ»	Дата-центр «Парковий» Телекомунікації, безпека
22	Департамент інформації та цифрових рішень Одеської міської ради	Державна установа
23	Комунальне підприємство «Теплопостачання міста Одеси»	Державна установа
24	Дочірнє підприємство «Фірма «Емералд Моторс»	Офіційний дилерський центр BMW
25	Приватне акціонерне товариство «Київстар»	Телекомунікаційний оператор
26	Управління поліції охорони в Одеській області	Національна поліція
27	Комунальне підприємство «Обласний інформаційно-аналітичний центр»	Державна установа
28	Громадська організація «Центр тактичної підготовки»	Інформаційна та практична діяльність у галузі безпеки і оборони

### **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: характеристика з місця проходження практики з рекомендованою оцінкою та звіт

### 4. 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 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		Н а р а х у в а н н я б а л і в	Бали нараховуються таким чином:  <i>Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою</i>
		для іспиту	для заліку		
90-100	A	Відмінно	зараховано		
82-89	B	Добре			
74-81	C				
64-73	D				
60-63	E	Задовільно			
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
<b>Відмінно (А) – від 90 до 100 балів</b>	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
<b>Дуже добре (В) – від 82 до 89 балів</b>	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.
<b>Добре (С) – від 74 до 81 балів</b>	Є зауваження щодо змісту та оформлення звіту й щоденника. У відповідях на запитання членів комісії з програми практики студент припускається окремих неточностей, хоча загалом має достатні знання.
<b>Задовільно (D) – від 64 до 73 балів</b>	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.
<b>Задовільно (Е) – від 60 до 63 балів</b>	Неповне опанування програмного матеріалу, але з відповіді якого слідує, що отримані ним знання і набуті практичні навички відповідають мінімальним критеріям оцінювання.
<b>Незадовільно з можливістю повторного складання (FX) – від 35 до 59 балів</b>	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
<b>Незадовільно з обов'язковим повторним вивченням дисципліни (F) – від 0 до 34 балів</b>	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\(suitt.edu.ua\);](http://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.