ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

29 серпня 2025 р.

РОБОЧА ПРОГРАМА ВИРОБНИЧОЇ ПРАКТИКИ 2

Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Рівень вищої освіти	Перший (бакалаврський)
Освітньо-професійна програма	Кібербезпека та захист інформації
Обсяг дисципліни	5 кредитів ЄКТС
Шифр дисципліни	ОПП.16
Мова навчання	Українська
Статус дисципліни	Обов'язкова (професійної підготовки)
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма здобуття освіти	Курс	Семестр	Обсяг практики		Вид семестрового контролю
			Кредити ЄКТС	Години	Залік (диференційований)
Д	4	8	5	150	+

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» за спеціальністю 125 «Кібербезпека та захист інформації»

Робоча програма складена _____ канд. техн. наук, доцент Віктор ЧЕШУН
Підпис(и) автора(ів) Науковий ступінь, учене звання Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 29.08.2025 № 1. Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувач кафедри, канд. техн. наук, доц.	Кібербезпеки		Юрій КЛЬОЦ
Гарант освітньо-професійної програми, канд. техн. наук, доц.	Кібербезпеки		Віктор ЧЕШУН

3 ПОЯСНЮВАЛЬНА ЗАПИСКА

Виробнича практика № 2 є одним із обов'язкових освітніх компонентів і займає провідне місце у фаховій підготовці здобувачів першого (бакалаврського) рівня вищої освіти очної (денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Кібербезпека та захист інформації» в межах спеціальності 125 «Кібербезпека та захист інформації».

Пререквізити: ОПП.06 Захист інформації в інформаційно-комунікаційних системах; ОПП.07 Безпека вебресурсів; ОПП.09 Прикладна криптологія; ОПП.12 Технології виявлення вразливостей та вторгнень; ОПП.13 Управління інформаційною безпекою; ОПП.14 Комплексні системи захисту інформації; ОПП.15 Виробнича практика 1.

Кореквізити: -.

Відповідно до освітньої програми практика сприяє забезпеченню:

***компетентностей*:** ІК Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов; ЗК 1 Здатність застосовувати знання у практичних ситуаціях; ЗК 2 Знання та розуміння предметної області та розуміння професії; ЗК 3 Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово; ЗК 4 Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; 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 2 Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки; ФК 3 Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах; ФК 4 Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки; ФК 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки; ФК 6 Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження; 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 10 Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності; ФК 11 Здатність виконувати моніторинг процесів функціонування інформаційних, 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 з встановленою політикою інформаційної та/або кібербезпеки.

***програмних результатів навчання*:** ПРН 1 Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН 2 Організовувати 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 частої 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 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/або кібербезпеки; ПРН 10 Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; ПРН 11 Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; ПРН 12 Розробляти моделі загроз та порушника; 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 15 Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; ПРН 16 Реалізовувати комплексні системи захисту

інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; ПРН 17 Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; ПРН 18 Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; ПРН 19 Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; ПРН 20 Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; 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 23 Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; ПРН 24 Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); 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 26 Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; ПРН 27 Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; 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 30 Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; 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/або кібербезпеки відповідно до цілей і завдань організації; ПРН 35 Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки; ПРН 36 Виявляти небезпечні сигнали технічних засобів; 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 39 Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; ПРН 40 Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; ПРН 41 Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; ПРН 42 Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; ПРН 43 Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів; ПРН 44 Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; ПРН 45 Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; 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; ПРН 48 Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; ПРН 49 Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; ПРН 50 Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); ПРН 51 Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; ПРН 52 Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; ПРН 53 Вирішувати задачі

аналізу програмного коду на наявність можливих загроз; ПРН 54 Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Мета практики. Закріплення теоретичних знань та удосконалення умінь, набутих у процесі теоретичного навчання; завершення формування у випускника професійних практичних навичок, необхідних для роботи на об'єктах працевлаштування.

Завдання практики:

– удосконалення умінь, навичок та практичних компетентностей із захисту інформації, безпечної поведінки в цифровому середовищі та розвитку кіберграмотності;

– поглиблення і закріплення теоретичних знань щодо здійснення фахової діяльності у сфері інформаційної безпеки та/або кібербезпеки;

– адаптація до умов фахової діяльності, розвиток необхідних для сучасного ринку праці навичок Soft skills.

Результати навчання. Після проходження другої виробничої практики здобувач вищої освіти повинен вміти використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; 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; діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки; готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки, приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; 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; розробляти моделі загроз та порушника; впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

4 ЗМІСТ ТА ОРГАНІЗАЦІЯ ПРАКТИКИ
4.1 Зміст практики

Зміст виробничої практики №2 відповідає освітньо-професійній програмі «Кібербезпека та захист інформації» першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації».

Практиканти працюють над завданнями, наведеними в програмі практики, використовуючи знання, набуті під час підготовки за спеціальністю, формують практичні навички щодо порядку проведення робіт із захисту інформації відповідно до законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

Орієнтовний календарний графік проходження виробничої практики №2 представлений у таблиці 1.

Таблиця 1. Орієнтовний календарний план практики

№ п/п	Зміст роботи	Кількість, днів
1	**Організаційний етап**	
1.1	Участь в установчих зборах. Ознайомлення із завданнями і програмою виробничої практики №2, правами та обов'язками студентів під час проходження практики.	1
1.2	Проходження інструктажу з техніки безпеки.	
1.3	Ознайомлення з базою практики та її організаційною структурою.	
1.4	Складання і погодження з керівником від бази практики індивідуального плану роботи на час практики.	
2	**Виконання завдань за планом практики**	
2.1	Вивчення інформаційної діяльності бази практики, визначення об`єктів захисту (інформаційних активів, технічного обладнання, інформаційно-комунікаційних систем і мереж, тощо).	3
2.2	Визначення і погодження з керівниками практики цільового об`єкта (об'єктів) захисту для виконання завдання виробничої практики №2.	7
2.3	Аналіз вразливостей об`єкта захисту та загроз його інформаційній безпеці.	
2.4	Розробка моделі загроз та порушника.	
2.5	Оцінювання ризиків можливості реалізації потенційних загроз інформації.	
2.6	Огляд-аналіз існуючих рішень та практик щодо протидії загрозам інформаційній безпеці об`єкта захисту (консультування з керівниками практики та фахівцями на базі практики; пошук, аналіз та синтез інформації з різних джерел).	3
2.7	Формулювання пропозицій щодо забезпечення інформаційної та/або кібербезпеки об`єкта захисту.	3
3	**Підсумки виробничої практики №2**	
3.1	Оформлення звіту та ведення щоденника практики згідно з вимогами, погодження матеріалів звіту з керівниками практики.	протягом практики
3.2	Формулювання висновків за результатами практики, завершення роботи над звітом і щоденником практики.	1
3.3	Подання звітної документації керівнику від бази практики	
3.4	Подання звітної документації на кафедру	
	Всього:	**18**

На основі орієнтовного тематичного плану, особливостей бази практики, особистих професійних інтересів здобувача вищої освіти складається індивідуальний план проходження практики. Подальше керівництво практикою, контроль за її виконанням здійснюється спільно керівником від бази практики та керівником від кафедри.

Перед початком проходження практики здобувачі вищої освіти одержують від керівника практики від кафедри індивідуальні завдання, які вони повинні виконати в період проходження практики. Індивідуальні завдання розробляються з врахуванням побажань здобувача вищої освіти щодо майбутнього працевлаштування та умов роботи установ – баз практики.

Індивідуальне завдання видається з метою формування у практикантів, в першу чергу, навичок проведення наукових досліджень, а також навичок самостійної роботи, уміння використовувати теоретичні знання в конкретних видах діяльності, аналізувати і оцінювати рівень інформаційної безпеки бази практики на основі теоретичних знань, які вони одержали в навчальному закладі, надбання практикантами під час практики умінь та навичок самостійного розв'язання завдань, пов'язаних з використанням комп'ютерної техніки в своїй роботі, активізації діяльності, розширення їх світогляду.

Окремий час для написання і оформлення звіту з практики та ведення щоденника не передбачається, звітна документація готується по мірі виконання завдання під час проходження практики. Безпосередній керівник від бази практики надає практикантам допомогу в зборі необхідного матеріалу (бланки, документи, література, власне консультування та консультування з іншими фахівцями), контролює виконання програми практики.

Орієнтовна тематика індивідуальних завдань на практику:

1. Сегментація корпоративної мережі організації на основі рівнів довіри та функціонального призначення.
2. Розгортання та налаштування систем моніторингу мережевих атак.
3. Організація захищених каналів зв’язку для віддаленого доступу до ресурсів компанії.
4. Впровадження централізованої автентифікації та авторизації для доступу до мережевого обладнання.
5. Розробка політики безпеки та розгортання системи контролю підключення нових пристроїв до локальної мережі підприємства.
6. Оптимізація правил міжмережевого екранування за результатами аналізу трафіку.
7. Захист бездротового сегмента мережі з використанням посилених методів автентифікації.
8. Налаштування комплексної системи моніторингу цілісності та доступності мережевої інфраструктури.
9. Розробка та впровадження списків контролю доступу для фільтрації трафіку на мережевому рівні.
10. Створення системи автоматизованого розгортання оновлень безпеки в корпоративній мережі.
11. Впровадження єдиних політик безпеки для посилення захисту операційних систем на хостах компанії.
12. Побудова системи централізованого захисту інформаційних ресурсів підприємства від шкідливого програмного забезпечення.
13. Організація збору, зберігання та обробки журналів подій безпеки з різних джерел.
14. Налаштування засобів криптографічного захисту інформації на носіях кінцевих пристроїв.
15. Реалізація моделі розмежування прав користувачів на основі мінімально необхідних привілеїв.
16. Створення захищеного ізольованого середовища для виконання критичних бізнес-операцій компанії.
17. Розгортання системи обліку та контролю встановленого програмного забезпечення для організації.
18. Забезпечення захищеного віддаленого адміністрування серверної інфраструктури.
19. Впровадження засобів фільтрації запитів до корпоративних веб-додатків.
20. Забезпечення захищеного обміну даними через веб-інтерфейси з використанням сучасних протоколів шифрування.
21. Проведення аналізу вразливостей веб-ресурсів згідно з міжнародними стандартами безпеки.
22. Впровадження механізмів багатофакторної перевірки автентичності користувачів.
23. Організація захищеного резервного копіювання даних у віддалені сховища.
24. Розмежування прав доступу до ресурсів у хмарному середовищі.
25. Удосконалення конфігурації веб-серверів для мінімізації поверхні атаки.
26. Побудова інфраструктури керування відкритими ключами всередині організації.
27. Організація корпоративної системи безпечного зберігання паролів та облікових даних.
28. Впровадження механізмів перевірки цілісності документів за допомогою електронного підпису.
29. Створення системи для захищеної передачі великих обсягів даних.
30. Розробка та технічне впровадження регламентів управління життєвим циклом паролів.
31. Проведення технічного сканування мережі для виявлення слабких місць та застарілого програмного забезпечення.
32. Аналіз передачі даних у мережі на наявність конфіденційної інформації у відкритому вигляді.
33. Розробка алгоритмів дій технічного персоналу під час виявлення інцидентів безпеки.
34. Перевірка відповідності налаштувань активного обладнання внутрішнім регламентам безпеки.
35. Оцінка рівня обізнаності персоналу шляхом проведення практичних перевірок на стійкість до соціальної інженерії.
36. Аудит та вдосконалення фактичних прав доступу до файлових ресурсів компанії.
37. Формування пакету технічної документації для авторизації системи захисту інформації підприємства.
38. Автоматизація збору та аналізу конфігураційних файлів для контролю несанкціонованих змін.
39. Класифікація інформаційних активів та розробка технічних заходів щодо їх захисту.
40. Проєктування системи технічного захисту об'єктів та приміщень організації.
41. Організація системи контролювання доступу до серверних приміщень.
42. Впровадження технічних засобів моніторингу за використанням пристроїв друку.
43. Розробка політики і методичних матеріалів для проведення занять з безпечного використання корпоративних ресурсів.
44. Створення та тестування плану відновлення працездатності систем після критичних збоїв.

4.2 Бази практики

Загальні вимоги щодо баз практики визначаються Положенням про практичну підготовку здобувачів вищої освіти ХНУ.

Практика проводиться на підприємствах різних форм власності, в організаціях різних галузей економіки, в органах державної влади, наукових установах і організаціях, діяльність яких безпосередньо пов’язана із кібербезпекою

та/або захистом інформації, або в структурі яких є підрозділи/фахівці, що забезпечують кібербезпеку та/або захист інформації.

Практика здобувачів вищої освіти проводиться на базах, які відповідають меті, завданням, змісту практики, а також вимогам освітньо-професійної програми підготовки бакалаврів за спеціальністю 125 «Кібербезпека та захист інформації».

Підприємства, які використовуються як бази практики, повинні мати можливість забезпечити проходження практики та виконання індивідуальних завдань відповідно до програми практики. Вони мають відповідати таким вимогам:

– наявність структур, що відповідають освітній програмі і спеціальності, за якою здійснюється підготовка студента-практиканта;
– сучасне технічне обладнання, програмне забезпечення та системи зв'язку;
– можливість кваліфікованого керівництва практикою студентів;
– можливість надання студентам на час практики робочих місць;
– надання студентам права користування бібліотекою, лабораторіями, технічною та іншою документацією для виконання програми практики (крім інформації та джерел з обмеженим доступом, якщо інше не погоджено договірними документами університету з базою практики та умовами завдання практики);
– надання студентам можливості зібрати матеріал для оформлення звіту з практики;
– наявність житлового фонду (за необхідністю).

Перевага надається підприємствам, які мають можливість подальшого працевлаштування випускників. За наявності в університеті державних, регіональних замовлень на підготовку фахівців, перелік баз практик надають органи, які формували ці замовлення. При підготовці фахівців за цільовими договорами з підприємствами бази практики передбачаються у цих договорах.

Як бази практичної підготовки студентів можуть використовуватися регіональні навчально-науково-виробничі центри з окремих спеціальностей, які створені у провідних навчальних закладах, за умови, що їх матеріально-технічна база відповідає вимогам програми практики. Зокрема, базами практики від Хмельницького національного університету є:

– Науково-навчальний центр кібербеки ХНУ;
– Центр цифрових технологій ХНУ.

Варіанти пропозицій можливих регіональних баз практики:

– ТОВ X-CITY, м. Хмельницький;
– відділ протидії кіберзлочинам в Хмельницькій області департаменту кіберполіції Національної поліції Уряїни, м. Хмельницький;
– ТВ Сервіс ТОВ «Воля», м. Хмельницький;
– Хмельницька філія ВАТ «Укртелеком»;
– ДП «Новатор», м. Хмельницький;
– ТОВ «Хмельницькінфоком»;
– філія АТ КБ «Приватбанк»;
– філія Хмельницького обласного управління АТ «Ощадбанк».
– філія ПАТ АБ «Укргазбанк».

Перелік баз практики щорічно коректується і оновлюється кафедрою. З базами практики університет завчасно укладає договори на її проведення, тривалість дії договорів погоджується договірними сторонами. Кафедра заздалегідь визначає бази практики і розподіляє по них студентів, повідомляючи їх про це до початку практики.

Студенти можуть самостійно, за погодженням з кафедрою та керівництвом університету, підбирати для себе базу практики і пропонувати її для укладання договору. Самостійний вибір студентами бази практики має бути погоджений з керівництвом підприємства, обраного за базу практики, та з керівником практики від кафедри не пізніше, ніж за місяць до її початку. Цей термін є необхідним для забезпечення можливості проведення аналізу відповідності умов, що створюються на пропонованій базі практики, вимогам щодо організації виробничої практики №2 для студентів спеціальності, укладання договорів на її проведення і затвердження бази практики наказом університету. Кафедра дає згоду про проходження практики на таких базах лише за умови, що вони відповідають вимогам для проходження практики.

5 ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Для досягнення програмних результатів навчання під час виробничої практики використовуються такі методи навчання: словесні (пояснення, бесіда, консультування); практичні; контекстного навчання; взаємного навчання; частково пошукові, проблемні; методи роботи з літературними та інформаційними джерелами тощо.

6 ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТНОЇ ДОКУМЕНТАЦІЇ З ВИРОБНИЧОЇ ПРАКТИКИ №2

Після закінчення терміну виробничої практики №2 здобувач вищої освіти звітує про виконання її програми. ***Формою звітності є письмовий звіт і щоденник практики***.

Рекомендується складати **звіт про практику** за структурою, наведеною в табл. 2.

Таблиця 2 – Структура звіту з практики

Розділ	Кількість сторінок
Титульний аркуш	1
Індивідуальне завдання на практику	1
Зміст	1
Вступ	1-2
1 Загальна характеристика бази практики та/або її структурних підрозділів (структурного підрозділу тощо).	2-3
2 Ідентифікація об`єкта захисту, аналіз вразливостей та загроз його інформаційній безпеці.	7-9
3 Моделі загроз та порушника.	
4 Оцінювання ризиків можливості реалізації потенційних загроз інформації.	
5 Огляд-аналіз існуючих рішень та практик щодо протидії загрозам інформаційній безпеці об`єкта захисту.	3-4
6 Формулювання пропозицій щодо забезпечення інформаційної та/або кібербезпеки об`єкта захисту.	2-5
Висновки	1-2
Перелік джерел посилань	1-2
Додатки	копія додатку до наказу на практику, інші додаткові матеріали за потреби
Разом:	**20-30**

Перший аркуш звіту з практики є титульним, він містить підписи керівників практики від кафедри і від бази практики.

Другий аркуш має назву «Індивідуальне завдання на практику» і містить перелік індивідуальних завдань, які мають бути вирішені в ході проходження практики.

У «Вступі» необхідно зазначити суть та актуальність вирішених під час практики завдань.

У першому розділі необхідно надати характеристику організації, описуючи її структуру, сферу діяльності та особливості функціонування підрозділів, де безпосередньо проходила практика. Особлива увага приділяється технічним і організаційним питанням інформаційної безпеки, специфікації наявного мережевого обладнання, серверних потужностей та архітектури інформаційних систем підприємства.

Другий розділ присвячений визначенню та класифікації ключових інформаційних активів, які потребують захисту, таких як бази даних, конфіденційна документація чи критичні бізнес-процеси. На основі аналізу середовища функціонування необхідно виявити слабкі місця в технічних конфігураціях, програмному забезпеченні та/чи фізичній охороні, що можуть бути використані для несанкціонованого доступу або порушення цілісності та доступності інформації.

Третій розділ передбачає систематизацію виявлених небезпек шляхом побудови моделі загроз, де описуються можливі вектори атак на інформаційну систему та сценарії їх реалізації. Одночасно формується профіль потенційного порушника, в якому визначаються його тип (зовнішній чи внутрішній), рівень технічної підготовки, ймовірна мотивація та обсяг прав доступу, якими він може володіти для здійснення шкідливого впливу на об’єкт захисту.

У четвертому розділі проводиться аналітична робота з визначення ймовірності успішного здійснення загроз та оцінки масштабів їхнього впливу на діяльність організації. Використовуючи обрану методику оцінювання, необхідно ранжувати виявлені ризики за ступенем критичності, враховуючи потенційні фінансові, репутаційні та технічні втрати, що дозволить визначити пріоритетність впровадження майбутніх заходів безпеки.

П’ятий розділ містить критичний огляд наявних на підприємстві засобів захисту, включаючи аналіз ефективності встановленого програмного забезпечення, мережевих екранів та чинних політик безпеки. Необхідно порівняти поточний стан захищеності об’єкта з вимогами законодавства та кращими галузевими практиками, щоб виявити прогалини в системі захисту та обґрунтувати потребу в її модернізації або зміні підходів до безпеки.

На основі проведеного дослідження у завершальному шостому розділі формулюються конкретні практичні рекомендації, спрямовані на посилення захищеності інформаційних ресурсів та мінімізацію критичних ризиків. Пропозиції можуть охоплювати технічні аспекти, такі як впровадження нових інструментів чи зміна конфігурацій, а також організаційні заходи, що стосуються оновлення регламентів роботи персоналу та вдосконалення процесів реагування на інциденти тощо.

У висновках необхідно стисло сформулювати, що було зроблено підчас проходження практики і відзначити отримані результати.

В переліку джерел посилань наводиться перелік літератури та інших джерел, що були опрацьовані для виконання програми практики. Кількість джерел рекомендована в межах 20-30.

Додатки можуть містити акти обстеження бази практики, копії використаних документів, схеми або програмний код власної програмної/інженерно-технічної розробки, проміжні та допоміжні результати виконання індивідуального завдання тощо.

Оформлювати звіт потрібно відповідно до вимог стандартів СОУ 207.01:2025 «Текстові документи. Загальні вимоги та правила складання» і СОУ 207.02:2025 «Бібліографічний запис. Загальні вимоги та правила складання».

Щоденник практики є офіційним документом, який містить інформацію про вид практики, терміни її проходження та назву закладу освіти, в якому вона відбудеться. Усі дані мають бути завірені деканом факультету та скріплені печаткою. В щоденнику зазначається день прибуття здобувача вищої освіти на базу практики та дата завершення практики, що засвідчує керівник від бази практики підписом і печаткою.

Крім цього в щоденнику містяться календарний графік проходження практики і робочі записи здобувача вищої освіти, відгуки керівників від бази практики та від кафедри про результати проходження практики здобувачем вищої освіти. Відгук керівника від бази практики в щоденнику та оцінювання роботи здобувача під час практики підписується та скріплюється печаткою бази практики.

Здобувачі вищої освіти звітують про проходження практики перед комісією, призначеною завідуючим кафедрою, до складу якої входять керівник практики від кафедри, відповідальний за нормоконтроль, інші викладачі кафедри та (за можливості) керівник від бази практики. Комісія приймає звіт у здобувачів вищої освіти і призначає дату захисту не пізніше одного тижня після завершення практики.

До захисту здобувач готує доповідь з презентацією. Доповідь на захисті має презентувати основні результати практики та доповнюватися презентацією з 8-10 слайдів. Тривалість доповіді – 3-5 хв. Слайди презентації мають висвітлювати загальну характеристику бази практики та/або її складових, а також основні результати виконання завдання практики: ідентифіковані інформаційні активи або інші об’єкти захисту, виявленні вразливості та результати їх оцінювання, моделі загроз і порушника, пропозиції та рекомендації щодо підвищення рівня захищеності інформації на базі практики, а також результати проведеного за індивідуальним завданням дослідження. Вони мають бути чіткі за змістом, пронумеровані, логічно пов’язані з доповіддю, але не дублювати її.

7 ПОЛІТИКА ПРОХОДЖЕННЯ ПРАКТИКИ

Політика проходження практики визначається системою вимог, що передбачені чинними положеннями Університету про організацію освітнього процесу і практичну підготовку здобувачів вищої освіти. До проходження практики кафедра організовує проведення зборів здобувачів вищої освіти з питань проходження практики за участю її керівників від кафедри. На зборах проводиться загальний інструктаж щодо особливостей і порядку проходження практики, завдань практики; здобувачі вищої освіти отримують направлення на практику і щоденник практики, рекомендації щодо оформлення звітної документації тощо.

Здобувач вищої освіти має своєчасно прибути на базу практик і пройти інструктаж з техніки безпеки та охорони праці. Під час практики він має вчасно й у повному обсязі виконувати всі завдання, передбачені програмою практики та настановами її керівників, суворо дотримуватися правил техніки безпеки, охорони праці, виробничої санітарії та внутрішнього розпорядку бази практики.

Після закінчення періоду практики здобувач вищої освіти у призначений час має прилюдно захистити звіт з практики перед комісією. Письмовий звіт, підписаний керівником і скріплений печаткою бази практики, разом з щоденником практики здобувач вищої освіти подає керівнику практики від кафедри.

Під час оформлення звіту з практики здобувач вищої освіти має ***дотримуватися політики академічної доброчесності*** (заборонено списування, плагіат, використання штучного інтелекту без належного цитування).

У випадку невиконання здобувачем вищої освіти програми практики з поважної причини, деканат, за заявою здобувача та на основі представлених документів, розглядає питання щодо надання йому академічної відпустки.

Здобувач вищої освіти, який на підсумковому контролі із захисту звіту з практики отримав негативну оцінку або не виконав програму практики без поважних причин, відраховується з Університету за невиконання індивідуального навчального плану.

Підсумки практики підводяться на засіданні кафедри і обговорюються на засіданні вченої ради факультету не рідше одного разу на навчальний рік.

8 ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ВИРОБНИЧОЇ ПРАКТИКИ №2

Формою підсумкового контролю для практики є диференційований залік.

Оцінювання результатів виробничої практики №2 здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи може бути зарахований, якщо здобувач вищої освіти набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

Будь-які форми порушення академічної доброчесності під час оцінювання **не допускаються**.

Критерії оцінювання структурних елементів загальної оцінки з виробничої практики №2:

– *оцінка керівника практики від бази практики:* повнота виконання програми практики; відповідність звіту

реаліям бази практики; відношення практиканта до роботи, його дисциплінованість, самоорганізованість і ініціативність; практична значимість пропозицій практиканта; вміння працювати в колективі, рівень комунікабельності та інші особисті риси, що проявились під час практики; професійна компетентність і застосування теоретичних знань;

– *оцінка керівника практики від кафедри*: унікальність звіту за результатами перевірки рівня унікальності тексту; самостійність написання звіту та етика використання штучного інтелекту; повнота вирішення завдання і досягнення мети практики; відповідність виконання етапів практики строкам календарного графіка; змістовна та структурно-логічна якість звітної документації;

– *оцінка звіту з практики комісією:* відповідність оформлення звітної документації вимогам ДСТУ та положень ХНУ (нормоконтроль); використання інформаційних джерел; аналітичне опрацювання матеріалів практики;

– *оцінка комісією доповіді і презентації під час захисту практики:* Змістовність, структурованість і логічність доповіді; уміння лаконічно, чітко та переконливо презентувати результати; якість візуального супроводу (презентації);

– *оцінка комісією відповідей на запитання під час захисту практики:* повнота та чіткість відповідей, їх правильність**;** логічність та обґрунтованість відповідей; загальна культура відповідей та ділове мовлення.

Результати виконання завдань практики та її захисту оцінюються за 100-бальною накопичувальною шкалою (таблиця 3).

Таблиця 3 – Кількість балів за кожним із структурних елементів загальної оцінки (мінімум-максимум)

Оцінка керівника практики від бази практики	Оцінка керівника практики від кафедри	Оцінка комісією			Разом балів
		звіту з практики	доповіді і презентації під час захисту практики	відповідей на запитання під час захисту практики	
1	2	3	4	5	
18-30	15-25	9-15	9-15	9-15	60-100

Критерії та кількість балів оцінювання за кожним структурним елементом загальної оцінки з виробничої практики №2 зазначені в таблиці 4.

Таблиця 4 – Критерії та кількість балів оцінювання за кожним структурним елементом загальної оцінки за практику

Види оцінок і критерії оцінювання структурних елементів	**Кількість балів**
1 Оцінка керівника практики від бази практики	**18-30**
1.1 Повнота виконання програми практики:	3-5
– програму практики виконано повністю, усі заплановані завдання реалізовані в повному обсязі.	5
– програму практики виконано з окремими зауваженнями; – основні завдання реалізовані якісно, однак окремі пункти потребують уточнення чи доопрацювання, що не впливає на отримані результати критично.	4
– програму практики виконано на достатньому для зарахування рівні; – частина завдань залишилася виконаною неповністю або виконана поверхнево, але на достатньому для зарахування рівні.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
1.2 Відповідність звіту реаліям бази практики:	3-5
– звіт повністю відповідає реаліям бази практики, опис діяльності, виконаних завдань і результатів є достовірним, конкретним і підтвердженим фактичними матеріалами бази практики.	5
– звіт загалом відповідає реаліям бази практики, подано правдиву інформацію, але окремі аспекти описані без достатньої деталізації, не підтверджені фактичними матеріалами бази практики тощо.	4
– відповідність звіту реаліям бази практики часткова, але не містить неправдивої інформації, наявні неточності чи некритичні розбіжності між змістом звіту та фактичними умовами або видами діяльності на базі практики.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
1.3 Відношення практиканта до роботи, його дисциплінованість, самоорганізованість і ініціативність:	3-5
– практикант виявив відповідальне ставлення до роботи, високий рівень дисциплінованості, самоорганізованість і ініціативність, дотримувався встановленого розпорядку та вимог керівників практики.	5
– практикант загалом сумлінно ставився до виконання обов’язків і виконав всі поставлені завдання, але з незначними порушеннями термінів; – при виконанні окремих завдань проявляв недостатню організованість і/або ініціативність, іноді потребував нагадувань або додаткового контролю тощо, що не вплинуло на кінцеву якість	4

результатів виконання завдань.	
– практикант виявляв нестабільне ставлення до роботи, але не порушував правила трудового розпорядку і виконав всі поставлені завдання не менш як на достатньому рівні; – дисциплінованість та організованість були на середньому рівні, завдання виконувались без виявлення ініціативи; – спостерігалися порушення термінів або не завжди відповідальне виконання завдань.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
1.4 Практична значимість пропозицій практиканта:	3-5
– пропозиції мають практичну значимість, є обґрунтованими, реалістичними, базуються на глибокому аналізі діяльності бази практики та можуть бути впроваджені для підвищення ефективності роботи.	5
– пропозиції загалом доцільні, містять раціональні ідеї щодо покращення окремих аспектів діяльності, однак потребують подальшого опрацювання чи конкретизації для практичного впровадження.	4
– пропозиції мають обмежену практичну цінність; – пропозиції частково відповідають реаліям бази практики; – пропозиції сформульовані поверхнево або без достатнього обґрунтування.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
1.5 Вміння працювати в колективі, рівень комунікабельності та інші особисті риси, що проявились під час практики:	3-5
– практикант виявив високий рівень уміння працювати в колективі, ефективно взаємодіяв із працівниками бази практики, проявляв комунікабельність, толерантність і здатність до командної роботи, сприяв підтриманню позитивного мікроклімату.	5
– практикант загалом добре взаємодіяв із колективом, підтримував робочі стосунки, виконував спільні завдання, однак потребував допомоги в налагодженні комунікації чи координації дій.	4
– практикант частково володіє навичками командної роботи; – у взаємодії з колективом спостерігалися пасивність або труднощі , недостатня ініціативність у спільній діяльності.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
1.6 Професійна компетентність і застосування теоретичних знань:	3-5
– практикант продемонстрував високий рівень професійної підготовки, впевнено застосовує теоретичні знання на практиці, глибоко розуміє сутність професійних завдань, уміє обґрунтовувати власні рішення та робити аналітичні висновки.	5
– практикант показав достатній рівень професійної підготовки, теоретичні знання використовує у практичній діяльності, хоча окремі аспекти потребують більшої глибини або самостійності.	4
– практикант володіє базовими теоретичними знаннями, застосовує їх частково або з помилками, не завжди вміє поєднати теорію з практикою.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
2 Оцінка керівника практики від кафедри	**18-30**
2.1 Унікальність звіту за результатами перевірки рівня унікальності тексту*: ** як запозичення і плагіат не враховуються виявлені системою перевірки на плагіат сталі фразеологізми та словосполучення, а також типові елементи звіту, наявність яких зумовлена діючими вимогами*	3-5
– звіт не містить ознак плагіату, рівень унікальності тексту високий (90-100%), всі текстові та інші запозичення задекларовані належним чином.	5
– звіт не містить ознак плагіату, рівень унікальності тексту високий (75-89,99%), всі текстові та інші запозичення задекларовані належним чином.	4
– звіт не містить ознак плагіату, рівень унікальності тексту задовільний (60-74,99%), всі текстові та інші запозичення задекларовані належним чином; – в звіті зустрічаються окремі фрагменти (текстові, рисунки, статистичні та інші дані тощо), на джерела запозичення яких посилання не оформлені належним чином, але це не носить системний характер і запозичення не видаються автором звіту за власні напрацювання .	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
2.2 Самостійність написання звіту та етика використання штучного інтелекту (ШІ):	3-5
– звіт написаний самостійно і не містить ознак використання ШІ; – використання ШІ є обґрунтованим і належно задекларованим, генерація фрагментів звіту ШІ не носить систематичний характер (менше 10%), всі ШІ-результати не видаються автором за особисті, а використовуються за основу для критичного аналізу, авторської переробки та синтезу з інформацією з інших джерел.	5
– використання ШІ є обґрунтованим і належно задекларованим, не має за мету генерацію фрагментів звіту або їх генерація не носить систематичний характер (менше 10%) і всі ШІ-результати не видаються автором за особисті, але, в окремих випадках, не містять ознак	4

авторської переробки та синтезу з інформацією з інших джерел; – використання ШІ є належно задекларованим, генерація фрагментів звіту має систематичний характер (10-25%) і не завжди є обґрунтованою, але всі ШІ-результати не видаються автором за особисті, використовуються за основу для критичного аналізу, авторської переробки та синтезу з інформацією з інших джерел;	
– використання ШІ є належно задекларованим, генерація фрагментів звіту має систематичний характер (10-30%) і не завжди є обґрунтованою, всі ШІ-результати не видаються автором за особисті, але більшістю не містять ознак критичної авторської переробки та синтезу з інформацією з інших джерел; – використання ШІ частково (в окремих випадках) не є належно задекларованим, але всі ШІ-результати не видаються автором за особисті.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
2.3 Повнота вирішення завдання і досягнення мети практики:	3-5
– завдання виконано якісно і у повному обсязі, результати повністю відповідають меті практики.	5
– завдання виконано повністю, є окремі зауваження щодо прийнятих рішень, їх подання або обґрунтування, але виявлені недоліки не впливають на загальний результат щодо досягнення мети практики.	4
– завдання виконано на мінімально прийнятному рівні; – досягнення мети практики може бути зарахованим, але з зауваженнями.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
2.4 Відповідність виконання етапів практики строкам календарного графіка:	3-5
– усі завдання виконано в установлений строк, дотримано графік без відхилень.	5
– завдання виконано своєчасно з незначними відхиленнями від графіка, що не вплинули на якість роботи.	4
– є окремі порушення строків виконання, частину завдань завершено із запізненням.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
2.5 Змістовна та структурно-логічна якість звітної документації:	3-5
– звітна документація повністю відповідає задекларованій структурі, зміст послідовно, логічно і повністю розкриває хід виконання етапів практики і їх взаємозв'язок, демонструє обґрунтованість результатів і прийнятих рішень та досягнення мети практики.	5
– звітна документація загалом відповідає задекларованій структурі з окремими недоліками; зміст документації відображує хід виконання етапів практики, але бажаним є уточнення окремих етапів або їх взаємозв'язку; обґрунтованість результатів і/або прийнятих рішень є загальною або недостатньо демонструє досягнення мети практики.	4
– звітна документація частково відповідає задекларованій структурі; зміст документації відображує хід виконання етапів практики несистематизовано; обґрунтованість результатів і/або прийнятих рішень є недостатньою.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
3 Оцінка звіту з практики комісією	**9-15**
3.1 Відповідність оформлення звітної документації вимогам ДСТУ та положень ХНУ (нормоконтроль):	3-5
– звітна документація повністю відповідає вимогам ДСТУ та положень ХНУ, оформлені грамотно, усі елементи присутні.	5
– звітна документація повністю відповідає вимогам ДСТУ та положень ХНУ, усі елементи присутні, але зустрічаються окремі формальні недоліки оформлення або граматичні/орфографічні помилки.	4
– звітна документація частково відповідає вимогам, але невідповідність не є критичною для відхилення звіту від захисту; – спостерігається значна кількість граматичних/орфографічних помилок.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
3.2 Використання інформаційних джерел:	3-5
– результати практики обґрунтовані широким спектром даних з різноманітних джерел, на всі джерела є посилання в тексті.	5
– результати практики обґрунтовані широким спектром даних з різноманітних джерел, але на окремі джерела відсутні посилання в тексті (до 15%); – при використанні різноманітних джерел спостерігається необґрунтована тенденція до надання переваги джерелам одного типу (більше 50%).	4
– використано меншу за передбачену вимогами кількість джерел (до 25%); – відсутні посилання в тексті на 15-40% джерел; – використано всі джерела одного типу	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
3.3 Аналітичне опрацювання матеріалів практики:	3-5
– аналіз виконано глибоко, причинно-наслідкові зв'язки чітко визначені, висновки логічні та обґрунтовані.	5

– аналіз достатній, але деякі аспекти не розглянуті детально; – висновки не акцентовані на основних результатах (є надлишково-повними).	4
– аналіз наявний, але поверхневий; – висновки частково сформульовані або фрагментарні.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
4 Оцінка комісією доповіді і презентації під час захисту практики	**9-15**
4.1 Змістовність, структурованість і логічність доповіді:	3-5
– доповідь повністю розкриває усі поставлені та виконані завдання, всі основні результати представлені логічно та послідовно, висновки обґрунтовані.	5
– доповідь розкриває поставлені та виконані завдання достатньо, але деякі аспекти викладаються поверхнево або непослідовно.	4
– доповідь частково розкриває поставлені та виконані завдання; – окремі результати подані фрагментарно, логіка викладу порушена.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
4.2 Уміння лаконічно, чітко та переконливо презентувати результати:	3-5
– здобувач подає матеріал зрозуміло, логічно, переконливо, підтримує увагу аудиторії, використовує термінологію професійно, дотримується регламенту.	5
– подача матеріалу достатньо зрозуміла, але іноді спостерігається невпевненість або нестача термінологічної точності; – регламент дотримано з незначними порушеннями (до 20 % відведеного часу).	4
– подача матеріалу частково зрозуміла; – виступ місцями неструктурований, спостерігаються труднощі з термінологією; – порушення регламенту більше 20 % відведеного часу.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
4.3 Якість візуального супроводу (презентації):	3-5
– презентація повністю інформативна, наочна, грамотно оформлена, допомагає розкриттю матеріалу.	5
– презентація достатньо інформативна, але частково відволікає від основних результатів або неповністю відображає матеріал.	4
– презентація частково інформативна, мінімально-достатня для демонстрації основних результатів; – оформлення поверхневе, матеріал поданий фрагментарно, але є достатнім для демонстрації основних результатів.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
5 Оцінка комісією відповідей на запитання під час захисту практики	**9-15**
5.1 Повнота та чіткість відповідей, їх правильність:	3-5
– відповіді є повними, чіткими і правильними.	5
– відповіді є повними і правильними, але недостатньо чіткими; – відповіді більшістю є повними.	4
– окремі відповіді не є правильними; – відповіді є загалом правильними, але недостатньо чіткими і повними.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
5.2 Логічність та обґрунтованість відповідей:	3-5
– відповіді повністю аргументовані, логічні, демонструють глибоке розуміння теми питань та їх практичних аспектів, доповідач демонструє вміння обґрунтувати логіку прийнятих рішень.	5
– відповіді аргументовані загалом, але деякі моменти потребують уточнення або додаткового обґрунтування (розкриваються у відповідях на уточнюючі питання тощо), доповідач не завжди демонструє вміння обґрунтувати логіку прийнятих рішень.	4
– відповіді частково аргументовані, недостатньо розкриваються у відповідях на уточнюючі питання тощо; – спостерігаються неточності або поверхневий рівень розуміння; – доповідач не може обґрунтувати логіку прийнятих рішень.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
5.3 Загальна культура відповідей та ділове мовлення:	3-5
– відповіді впевнені, мова чітка, поведінка професійна і сприяє позитивному враженню.	5
– відповіді достатньо впевнені, але викликає зауваження ділове мовлення або професійна поведінка.	4
– відповіді місцями невпевнені; – невпевнена ділова мова; – поведінка частково професійна.	3
– за підкритерієм не досягнуто результатів, достатніх для отримання позитивної оцінки.	0
Сума:	**60-100**

Накопичена здобувачем вищої освіти сума балів за результатами виконання програми практики трансформується в інституційну шкалу оцінювання та шкалу оцінювання ЄКТС (таблиця 5).

Таблиця 5 – Співвідношення шкал оцінювання інституційної і ЄКТС

Оцінка ЄКТС	Рейтингова шкала балів	Інституційна оцінка (опис рівня досягнення здобувачем запланованих результатів навчання з освітнього компонента)	
		Залік	Іспит/диференційований залік
A	90–100	Зараховано	***Відмінно*/*Excellent*** – високий рівень досягнення запланованих результатів навчання з освітнього компонента, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом
B	83–89		***Добре*/*Good*** – середній (максимально достатній) рівень досягнення запланованих результатів навчання з освітнього компонента та готовності до подальшого навчання та/або професійної діяльності за фахом
C	73–82		
D	66–72		***Задовільно*/*Satisfactory*** – достатній рівень. Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з освітнього компонента
E	60–65		
FX	40–59	Незараховано	***Незадовільно*/*Fail*** – недостатній рівень. Низка запланованих результатів навчання з освітнього компонента відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом
F	0–39		***Незадовільно*/*Fail*** – результати навчання відсутні

Результати захисту звіту з виробничої практики №2 заносяться до заліково-екзаменаційної відомості та індивідуального навчального плану здобувача вищої освіти за двома шкалами оцінювання – інституційною та ЄКТС з підписами членів комісії.

9 НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Освітній процес з виробничої практики №2 забезпечений необхідними навчально-методичними матеріалами, що розміщені в Модульному середовищі для навчання MOODLE:

1. Курс «Виробнича практика 2»: https://msn.khmnu.edu.ua/course/view.php?id=10269

10 МАТЕРІАЛЬНО-ТЕХНІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ПРАКТИКИ

Інформаційна та комп'ютерна підтримка: ПК або ноутбук, доступ до мережі Інтернет, робота з презентаціями, проєктор на етапі захисту звіту.

Інше матеріально-технічне та програмне забезпечення практики залежить від бази практики та адаптованого до неї індивідуального плану проходження практики.

11 РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Положення про практичну підготовку здобувачів вищої освіти у Хмельницькому національному університеті. URL: https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-praktychnu-pidgotovku.pdf
2. Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у Хмельницькому національному університеті. URL: https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-kontrol-i-oczinyuvannya-rezultativ-navchannya-zdobuvachiv.pdf
3. Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті. URL: https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf
4. Текстові документи. Загальні вимоги та правила складання. СОУ 207.02:2025. / Синюк О.М. та ін. Хмельницький: ХНУ, 2025. 46 с. URL: https://gma.khmnu.edu.ua/wp-content/uploads/sites/20/text.pdf
5. Синюк О.М., Шмурікова О.П. Бібліографічний запис. Загальні вимоги та правила складання. СОУ 207.02:2025. Хмельницький : ХНУ, 2025. 37 с. URL: https://gma.khmnu.edu.ua/wp-content/uploads/sites/20/bibliografiya_2025.pdf
6. Кушнір М. Я., Цеханський В. Д. Законодавчі питання інформаційної безпеки: Електронний навчальний посібник. Чернівці : Чернівецький національний університет, 2024. 102 с. URL: https://drive.google.com/file/d/1r7JUzLpdq-RM2Oq-iDM_Uzk3nG4V2wAC/view
7. Правове регулювання національної безпеки : навчальний посібник / О. Г. Боднарчук та ін. Ірпінь: Державний податковий університет, 2024. 202 с. URL: https://dpu.edu.ua/images/Documents/NAUKA/Naukova%20biblioteka/Navcalno-

metodicna%20literatura/N/Pravove%20reguluvanna%20nacionalnoi%20bezpeki.pdf

8. Потенко О.С. Методи визначення функціонального профілю захисту автоматизованої системи з урахуванням поточного рівня загроз : дис. … канд. техн. наук : 05.13.21, Київ, 2024. 172 с. URL: https://ipme.kiev.ua/docs/Potenko/Dis_Potenko.pdf

9. Кримінально-правова охорона інформаційної безпеки в Україні: монографія / В. І. Борисов та ін.; за заг. ред. В. І. Борисова, О. О. Пащенка ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. 328 с. DOI: https://doi.org/10.31359/9786178518899.

10. Організаційно-правові основи забезпечення кібербезпеки / А. І. Марущак та ін. К.: Видавництво Ліра-К, 2023. 309 с.

11. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://izmail.maup.com.ua/biblioteka/akademichna-dobrochesnist2/dstu-8302-2015/prikladi-oformlennya-bibliografichnih-posilan-dstu-8302-2015 (дата звернення: 28.08.2025).

12. Безпека інформаційно-комунікаційних систем : підручник / Ю.В. Костюк, П.М. Складанний, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзаєва, М.В. Ворохоб. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 1016 с. https://elibrary.kubg.edu.ua/id/eprint/51358/1/Kostiuk_Y_Skladannyi_P_Bebeshko_B_Khorolska_K_Rzaieva_S_Vorokhob_M_BIKS_2025_FITM.pdf

13. Пашорін В. І., Костюк Ю. В. Безпека інформаційних систем : навч. посіб. Київ : Держ. торг.-екон. ун-т, 2023. 376 с. https://ur.knute.edu.ua/items/8fb49cdc-6a75-4685-ac9e-d7082aa8e6e3/full

14. Комплексна безпека інформаційних мережевих систем: навчальний посібник/ Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. Тернопіль: ФОП Паляниця В.А., 2023. 324 с. https://surl.li/twfduf

15. Ланде Д.В. OSINT у кібербезпеці: навч. пос. Київ: ТОВ «Інжиніринг», 2024. 522 с.

16. Хлапонін Ю.І. Комплексні системи захисту інформації: конспект лекцій. Київ: КНУБА, 2022. 84 с. URL: https://repositary.knuba.edu.ua/server/api/core/bitstreams/6b05fa85-b573-4300-ad40-45b63e198ffa/content

17. Комплексні системи захисту інформації : Навчальний посібник [Електронний ресурс] / Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. URL: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/ (дата звернення: 22.08.2025)

18. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. Навч. посіб./ В.М. Богуш, В. Д. Бровко, О.С. Кобус, В.Д. Козюра. Київ: Видавництво Ліра-К, 2023. 508 с.

19. Методи та засоби технічного захисту інформації. Опорний конспект лекцій навч. посіб. для здобувачів ступеня бакалавра за освітньою програмою «Системи технічного захисту інформації» спеціальності 125 «Кібербезпека» / уклад.: В. М. Луценко, Д. О. Прогонов. Київ : КПІ ім. Ігоря Сікорського, 2021. 289 с. URL: https://ela.kpi.ua/handle/123456789/42397

20. Технічні засоби захисту інформації: Опорний конспект лекцій з дисципліни для студентів освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні спеціальності 125 «Кібербезпека» / Укл.: Яцків В.В., Кулина С.В. Тернопіль 2023. 88 с. URL: https://dspace.wunu.edu.ua/bitstream/316497/49114/1/Технічні%20засоби%20захисту%20інформації.pdf

21. Онацький О. В., Йона Л. Г., Белова Ю. В. Криптографічний захист інформації: навч. посіб. Одеса: «Астропринт», 2023. 249 с. https://dspace.onua.edu.ua/items/38a4e463-fef8-4d39-a7a9-d82c4288c3ca

22. Гапак О.М. Криптоаналіз. Криптографічні протоколи : навчальний посібник. Ужгород: Ужгородський національний університет, 2021. 93 с. URL : https://dspace.uzhnu.edu.ua/items/e7568dd6-c6fc-45fa-a35e-d005155840f0

23. Живило Є.О. Тестування на проникнення: навч. посіб. Ч.1. Полтава : Нац. ун-т ім. Ю. Кондратюка, 2024. 134 с. https://reposit.nupp.edu.ua/handle/PoltNTU/15798

24. Живило Є.О. Тестування на проникнення: навч. посіб. Ч.2. Полтава : Нац. ун-т ім. Ю. Кондратюка, 2024. 239 с. URL : https://reposit.nupp.edu.ua/handle/PoltNTU/15799

25. Information Security Handbook / Noor Zaman Jhanjhi, Khalid Hussain, Mamoona Humayun, Azween Bin Abdullah, João Manuel R.S. Tavares. CRC Press, 2022. 250 p.

12 Інформаційні ресурси

1. Модульне середовище для навчання. URL: https://msn.khmnu.edu.ua/course/view.php?id=10269
2. Електронна бібліотека ХНУ. URL: http://library.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://elar.khmnu.edu.ua/home
4. Законодавство України. Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws
5. ISO Standards. Офіційний портал ISO – International Organization for Standardization. URL: https://www.iso.org/standards.html