МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Фаховий коледж інженерії, управління та землевпорядкування
Державного некомерційного підприємства
«Державний університет «Київський авіаційний інститут»

ПОГОДЖЕНО
Завідувач навчально-виробничої практики
_____/Андрій ПОНОМАРЕНКО/
«27» 08 2025 р.

ЗАТВЕРДЖЕНО
Заступник директора
з навчально-методичної роботи
_____/Альона ХЕБДА/
«27» 08 2025 р.

НАСКРІЗНА ПРОГРАМА ПРАКТИЧНОЇ ПІДГОТОВКИ

Галузь знань: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма: «Кібербезпека»
Освітньо-професійний ступінь фаховий молодший бакалавр

КИЇВ
2025-2026 н.р.

Наскрізну програму практичної підготовки розроблено на основі освітньо-професійної програми «Кібербезпека», навчальних планів підготовки за денною формою здобувачів фахової передвищої освіти освітньо-професійного ступеня «Фаховий молодший бакалавр» за спеціальністю 125 «Кібербезпека та захист інформації»

РОЗРОБНИКИ ПРОГРАМИ

Викладач вищої категорії _____ Ганна КРАЛІНА
(підпис) (Ім'я ПРІЗВИЩЕ)

Обговорено на засіданні циклової комісії інформаційних технологій та електронних комунікацій
(назва комісії)

Протокол № 1 від «26» 08 2025р.

Голова циклової комісії інформаційних технологій та електронних комунікацій
(назва комісії)

_____ Ганна КРАЛІНА
(підпис) (Ім'я ПРІЗВИЩЕ)

Робочу програму наскрізної програми практичної підготовки практики обговорено та схвалено на засіданні Науково-методичної ради Протокол № 1 від «27» 08 2025р.

Голова НМР _____ Альона ХЕБДА
(підпис) (Ім'я ПРІЗВИЩЕ)

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Наскрізна програма практичної підготовки здобувачів освіти повинна сприяти забезпеченню якісної теоретичної підготовки випускників, формуванню в них професійних практичних знань, умінь та навичок, необхідних для майбутньої праці, вивченню основ організаторської та управлінської діяльності.

Наскрізна програма практичної підготовки є однією з основних форм навчального процесу, спрямована на формування й виховання висококваліфікованого фахівця. Основним навчально-методичним документом, що визначає проведення практики, що регламентує навчальну діяльність студентів і діяльність викладача на практиці, є наскрізна програма практичної підготовки. Наскрізна програма практичної підготовки забезпечує єдиний комплексний підхід до організації практичної підготовки, системності, безперервності й наступності навчання студентів. Наскрізна програма забезпечує єдиний комплексний підхід до організації виробничої практичної підготовки, системності, безперервності та спадкоємності навчання здобувачів освіти. Наскрізна програма є основою для складання робочих програм практики, що враховує особливості баз практики й конкретні умови проходження практики.

Наскрізна програма практичної підготовки складена з урахуванням видів практик та їх тривалості.

Наскрізна програма практичної підготовки розрахована на весь період навчання, містить види і тривалість навчальної та виробничих практик, які перераховані в таблиці 1.

Таблиця 1

Перелік видів виробничої практики

Вид практики	Семестр проведення	Тривалість (годин)
Навчальна практика	4 семестр	180
Виробнича (технологічна) практика	6 семестр	270
Виробнича практика	8 семестр	270

1.1 Мета практичної підготовки

Практичне навчання займає важливе місце в вирішенні завдання підготовки висококваліфікованих спеціалістів, які володіють комплексом професійних знань, практичними навичками програмування і документування та необхідними організаторськими якостями.

Практичне навчання здобувачів освіти є одним з найважливіших етапів навчального процесу, метою якого є закріплення, поглиблення та систематизація знань з професійно-орієнтованих дисциплін, набуття професійних вмінь і навичок зі спеціальності, долучення студентів до праці та вміння працювати у колективі.

Метою практики є:

– закріплення та поглиблення знань і вмінь, отриманих здобувачами освіти в процесі навчання, а також оволодіння системою професійних вмінь, навичок та початковим досвідом професійної діяльності;

– формування вмінь і навичок, необхідних для розв'язання конкретних прикладних задач, які виникають в процесі діяльності підприємств різного типу;

– отримання навичок аналізу інформаційної системи управління, що функціонує на об'єкті, з метою його розвитку та покращення на підставі застосування нових інформаційних технологій та сучасних інструментальних засобів.

1.2 Завдання практичної підготовки

Практика покликана сформувати у здобувача освіти професійні вміння, навички прийняття самостійних рішень на конкретній ділянці роботи в реальних виробничих умовах шляхом виконання обов'язків, властивих їх майбутньої професійної діяльності.

Поставлені цілі реалізують шляхом самостійного вивчення виробництва й виконання кожним здобувачем освіти в умовах підприємства необхідних програмою окремих виробничих завдань.

Завданнями практики є:

– забезпечення зв'язка практичного навчання з теоретичним;

– придбання практичних знань і навичок за фахом;

- ознайомлення із заходами щодо підвищення продуктивності праці, автоматизації бізнес-процесів, та реінжинірингу бізнес-систем;
- ознайомлення з питаннями організації, планування й економіки виробництва на даному підприємстві;
- дотримання вимог техніки безпеки та стандартів інженерної діяльності;
- формування навичок роботи в команді та дотримання професійної етики у сфері кібербезпеки.
- придбання навичок у винахідницькій й раціоналізаторській роботі;

1.3 Організація практики

Навчально-методичне керівництво з урахуванням видів практик здійснюють викладачі циклової комісії відповідно до навчального навантаження.

Відповідальний за проведення практики вчасно доводить до здобувача освіти інформацію щодо баз практики. Здобувачі освіти у зазначений термін подають заяву з зазначенням бази практики що обрана.

Офіційною підставою для проведення виробничої практики здобувачів освіти на виробництві є договір, який укладається між коледжем та підприємством.

Керівник підприємства-бази практики видає наказ, де визначає порядок організації та проведення практики, заходи щодо створення необхідних умов студентам-практикантам для виконання ними програми практики, щодо охорони праці та запобігання виникнення нещасних випадків, контролю за виконанням студентами правил внутрішнього трудового розпорядку, інші заходи, призначає керівника практики від підприємства.

Перед початком практики відповідальний за проведення практики проводить виробничу нараду студентів-практикантів та викладачів – керівників практики для роз'яснення мети, змісту та порядку проходження практики.

За місяць до практики відповідальний за проведення практики оформлює наказ про практику з вказівкою керівників.

На основі наказу викладач, відповідальний за практику формує графік відвідувань керівниками здобувачів освіти на їх робочих місцях з метою надання консультацій та контролю проходженням практики.

Перед відправкою до бази практики здобувач освіти повинен одержати щоденник практики, програму її проходження, індивідуальне завдання за дипломним та курсовим проєктом.

У період проходження практики здобувач освіти повинен:

- виконувати завдання, передбачені програмою практики та календарним графіком;
- підпорядковуватися діючим правилам внутрішнього трудового розпорядку підприємства;
- суворо дотримуватися правил техніки безпеки та охорони праці;
- працювати на робочому місці, яке вказано керівником практики від підприємства і нести відповідальність за виконану роботу та її результати нарівні зі штатними робітниками;
- систематично вести щоденник проходження практики.

1.4 Бази практичної підготовки

Навчальна практика проводиться на базі коледжу в спеціалізованих лабораторіях.

Виробничі практики проводяться на підприємствах, в організаціях, науково-дослідницьких інститутах, банках, страхових компаніях та інших установах, що займаються проєктуванням, упровадженням та експлуатацією автоматизованих інформаційних систем та інших програмних продуктів.

Базами практики рекомендується обирати підприємства, які мають договір з коледжем про підготовку для них фахівців.

До участі у проведенні виробничої практики залучаються підприємства та організації, які використовують сучасні засоби та інструментарій розробки та створення програмної продукції, яка застосовується в різних сферах діяльності.

Здобувачі освіти можуть самостійно підбирати для себе місця проходження практики та пропонувати їх для використання.

Закріплення баз практики проводиться згідно до встановленого порядку міністерства освіти і науки України.

Тривалість дії договорів узгоджується сторонами договорів та може бути

визначена на період конкретного виду практики.

Бази практики повинні:

– мати високий рівень техніки та технології, організації та культури праці, сучасну обчислювальну техніку та інформаційні технології;

– забезпечувати можливість поступового проведення технологічної, виробничої, та переддипломної практики за умови дотримання прийнятності їх робочих програм.

Функції підприємства-бази практики:

– забезпечувати якісне проведення інструктажу з пожежної безпеки охорони праці, техніки безпеки та промислової санітарії;

– надавати згідно з робочою програмою здобувачам освіти місця практики, які забезпечують найбільшу ефективність її проходження;

– створювати необхідні умови для одержання здобувачами освіти в період проходження практики знань за спеціальністю;

– дотримуватись календарного графіку проходження практики;

– надавати студентам-практикантам можливість користуватися літературою, проєктною, техніко-економічною та іншою документацією;

– надавати допомогу при підборі матеріалів для курсових проєктів;

– забезпечувати та контролювати дотримування студентами-практикантами правил внутрішнього трудового розпорядку, які встановлені для конкретного підприємства, у тому числі час початку та закінчення роботи.

Безпосереднє керівництво виробничою практикою покладається за наказом керівника підприємства на провідних спеціалістів структурних підрозділів.

1.5 Керівництво та контроль за проходженням практики

Викладач, відповідальний за проведення практики:

– забезпечує якісне виконання програми практики та високу якість її проведення;

– призначає керівниками виробничої практики досвідчених викладачів;

– розподіляє на основі укладених з підприємством договорів здобувачів освіти за базами практики;

– призначає старшого з групи здобувачів освіти, які проходять практику на одному підприємстві;

– забезпечує підприємство, а також самих практикантів програмами практики;

– здійснює суворий контроль за організацією та проведенням виробничої практики здобувачів освіти на підприємстві, і дотримуванням строків та змісту.

Обов'язки керівника практики від коледжу:

– забезпечити проведення всіх організаційних заходів перед відправкою здобувачів освіти на практику;

– забезпечити високу якість проходження практики і сувору відповідальність її навчальному плану й програмі;

– надавати консультації здобувачам освіти з усіх питань практики;

– контролювати додержання студентами-практикантами правил внутрішнього розпорядку;

– здійснювати поточний контроль проходження практики у відповідності із календарним графіком;

– розглядати звіти здобувачів освіти з практики, надавати відгук та висновок з практики та звіту.

В обов'язки керівника практики від підприємства входить:

– познайомити здобувачів освіти з організацією праці на конкретному робочому місці;

– здійснювати постійний контроль за виробничою роботою практикантів, допомагати їм вірно виконувати всі завдання на даному робочому місці, консультувати по виробничих питаннях;

– контролювати ведення щоденників, підготовку звітів студентами-практикантами та складати на кожного здобувача освіти виробничу характеристику-відгук керівника практики від підприємства.

1.6 Оформлення та захист звіту

У ході практики здобувач освіти повинен скласти письмовий звіт, підписати його у керівника практики від підприємства, поставити печатку і разом з оформленим відповідним чином щоденником практики, характеристикою-відгуком від

підприємства здати керівнику практики від коледжу.

Звіт з практики складається після збору матеріалів та виконання розділів програми, його оформлення закінчується на підприємстві до моменту закінчення практики.

Додаток до звіту складається з форм зібраних первинних документів, вихідних машинограм, схем та програм.

Захист здобувачем освіти звіту здійснюється перед керівником практики від коледжу.

2. ПРОГРАМИ ОКРЕМИХ ВИДІВ ПРАКТИК

2.1 Навчальна практика

Навчальна практика для здобувачів освіти спеціальності 125 «Кібербезпека та захист інформації» проводиться на ІІ курсі у 4 семестрі. Тривалість навчальної практики – чотири тижні, кількість кредитів – 6 (180 годин), форма підсумкового контролю – залік (захист звітів по практиці).

Мета навчальної практики освітньо-професійної програми «Кібербезпека» полягає у формуванні у здобувачів освіти базових професійних компетентностей у сфері захисту інформації, закріпленні теоретичних знань та набутті практичних навичок застосування сучасних технологій і методів забезпечення інформаційної безпеки.

Завдання навчальної практики:

– ознайомлення з принципами організації систем захисту інформації;

– формування навичок роботи з операційними системами, мережами та засобами кіберзахисту;

– набуття практичного досвіду виявлення, аналізу та попередження кіберзагроз;

– засвоєння основ адміністрування інформаційних систем та мереж;

– розвиток умінь використовувати інструменти моніторингу, тестування вразливостей і реагування на інциденти;

– дотримання вимог техніки безпеки та стандартів інженерної діяльності;

– формування навичок роботи в команді та дотримання професійної етики у сфері кібербезпеки.

У результаті проходження навчальної практики здобувачі освіти повинні вміти застосовувати отримані знання для розв'язання типових задач у сфері кібербезпеки та бути готовими до подальшого професійного навчання і практичної діяльності.

Компетентності та результати навчання.

Результати навчання, які дає можливість досягти навчальна практика.

РН03. Використовувати результати самостійного пошуку, аналізу та синтезу інформації різних джерел для ефективного рішення спеціалізованих задач

професійної діяльності.

РН04. Аналізувати, аргументувати, приймати рішення при розв'язанні типових спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН06. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

РН11. Аналізувати проєкти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

РН12. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно- телекомунікаційних системах програмно-апаратними засобами, та давати оцінку якості прийнятих рішень.

РН14. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН16. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

РН19. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

РН22. Організовувати процес свого навчання та самоосвіти.

Компетентності, які дає можливість здобути навчальна практика:

Загальні:

ЗК01. Здатність застосовувати знання у практичних ситуаціях.

ЗК05. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Спеціальні (Фахові):

СК05. Здатність забезпечувати захист інформації, що обробляється В інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК07. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації

СК09. Здатність здійснювати професійну діяльність на основі впровадженої

системи управління інформаційною безпекою.

Міждисциплінарні зв'язки навчальної практики освітньо-професійної програми «Кібербезпека» забезпечують інтеграцію знань із різних навчальних дисциплін та сприяють формуванню комплексного підходу до вирішення професійних завдань у сфері захисту інформації. Навчальна практика виступає інтегруючим елементом, що поєднує теоретичні знання з різних дисциплін і забезпечує їх практичне застосування для розв'язання комплексних задач у сфері кібербезпеки.

Навчальна практика проводиться на базі Фахового коледжу інженерії, управління та землевпорядкування Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут».

Зміст навчальної практики студентів зі спеціальності «Кібербезпека та захист інформації» передбачає послідовне ознайомлення здобувачів освіти з організацією практики, її метою, завданнями та вимогами, проведення інструктажу з охорони праці та техніки безпеки, а також отримання індивідуальних завдань. У процесі практики студенти поглиблюють знання з основ кібербезпеки, аналізують сучасні кіберзагрози та типові сценарії атак, оцінюють ризики та визначають вразливості інформаційних систем. Значна увага приділяється практичним навичкам захисту операційних систем, зокрема налаштуванню облікових записів, політик безпеки, оновленню програмного забезпечення та аналізу журналів подій. Студенти також опановують методи забезпечення мережевої безпеки через дослідження структури комп'ютерних мереж, аналіз мережевих протоколів, налаштування брандмауерів і моніторинг мережевого трафіку. Важливим складником є використання криптографічних методів захисту інформації, зокрема шифрування даних і забезпечення їх конфіденційності та цілісності. У ході практики здобувачі освіти застосовують інструменти для виявлення вразливостей, здійснюють базове тестування безпеки та аналізують стан захищеності інформаційних систем. Окремий етап присвячено реагуванню на кіберінциденти, включаючи їх виявлення, аналіз причин та розробку заходів щодо усунення наслідків і запобігання повторним порушенням. Завершальним етапом є виконання індивідуального завдання або мініпроєкту, оформлення результатів у вигляді звіту, ведення щоденника практики, формулювання висновків і рекомендацій, а також захист результатів практики з подальшим оцінюванням рівня сформованих

професійних компетентностей.

У результаті проходження навчальної практики студент спеціальності «Кібербезпека та захист інформації» повинен набути та продемонструвати сформовані загальні та фахові компетентності, що забезпечують готовність до виконання професійних завдань у сфері захисту інформації. Здобувач освіти повинен знати основні принципи та методи забезпечення кібербезпеки, типи сучасних кіберзагроз і способи протидії їм, основи функціонування операційних систем і комп'ютерних мереж, а також базові криптографічні підходи до захисту даних. Студент має вміти налаштовувати базові параметри безпеки операційних систем, керувати доступом користувачів, здійснювати моніторинг систем і мереж, виявляти потенційні вразливості та аналізувати інциденти безпеки. Важливим результатом є здатність застосовувати інструменти тестування безпеки, працювати з програмними засобами кіберзахисту, забезпечувати конфіденційність, цілісність і доступність інформації. Крім того, студент повинен уміти документувати результати своєї діяльності, готувати звітну документацію, презентувати отримані результати та аргументовано їх захищати. У підсумку здобувач освіти має продемонструвати готовність до подальшого професійного навчання і виконання типових завдань у сфері кібербезпеки, а також здатність працювати як самостійно, так і в команді.

Календарний графік проходження практики містить етапи робіт, які студент повинен освоїти в процесі проходження практики, із зазначенням їх тривалості (табл. 1).

Таблиця 1 – Орієнтовний календарний графік проходження практики

№ п/п	**Назва етапу**	**Кількість днів/тижнів**
1.	Інструктаж з техніки безпеки та правила протипожежної безпеки під час роботи в комп'ютерній лабораторії.	Початок практики
2.	Закріплення робочих місць за кожним здобувачем освіти в комп'ютерних лабораторіях.	Початок практики
3.	Виконання індивідуального завдання.	1-3 тиждень
4.	Оформлення звіту згідно методичних рекомендацій та його захист	4 тиждень

Таблиця 2 – Тематичний план навчальної практики

№ з\п	Тема	К-ть годин
1.	Вступ. Інструктаж з техніки безпеки. Аналіз апаратного та програмного забезпечення, встановленого на робочому місці в комп'ютерній лабораторії. Ознайомлення з програмою практики, правилами безпеки, організацією роботи	12
2.	Основи кібербезпеки та загрози. Вивчення типів кіберзагроз, аналіз атак, основні принципи захисту.	18
3.	Операційні системи та їх захист	12
4.	Налаштування безпеки ОС, управління користувачами, політики доступу	18
5.	Комп'ютерні мережі та мережева безпека	12
6.	Аналіз мережевих протоколів, налаштування брандмауера, моніторинг трафіку	12
7.	Криптографічний захист інформації	6
8.	Основи шифрування, використання криптографічних інструментів	12
9.	Виявлення вразливостей.	12
10.	Використання інструментів сканування, аналіз вразливостей систем	12
11.	Реагування на інциденти	18
12.	Моделювання кіберінцидентів, розробка заходів реагування	18
13.	Систематизація матеріалів, оформлення звітів і залік з навчальної практики	18
	Всього	**180**

2.2 Технологічна практика

Технологічна практика для здобувачів освіти спеціальності 125 «Кібербезпека та захист інформації» проводиться на III курсі у 6 семестрі. Тривалість технологічної практики – шість тижнів, кількість кредитів – 9 (270 годин), форма підсумкового контролю – залік (захист звітів по практиці).

Метою технологічної практики є:

– систематизація, закріплення і розширення теоретичних і практичних знань здобувачів освіти, набутих в попередні періоди навчання;

– формування у студентів, на базі здобутих під час навчання знань, професійних умінь і навичок для прийняття самостійних рішень під час конкретної роботи в реальних ринкових і виробничих умовах;

– оволодіння сучасними методами, формами організації та знаряддями праці, виховання потреби систематично поновлювати свої знання та творчо застосовувати їх у практичній діяльності;

– поглиблення та закріплення знань, які одержали студенти під час теоретичної підготовки, також оволодіння сучасними формами та методами роботи з комплексом задач, розв'язуваних на підприємстві з використанням комп'ютерної техніки та інформаційних технологій;

– набуття необхідних навичок у здійсненні операцій технологічного процесу обробки інформації;

– формування професійних вмінь і навичок у оцінці рівня безпеки інформаційних систем;

– виховання потреби систематичного оновлення своїх знань та їх творчого застосування у практичній діяльності.

– формування професійних навичок застосування сучасних технологій захисту інформації;

– набуття досвіду роботи з програмними та апаратними засобами кіберзахисту;

– набуття досвіду виявляти та усувати вразливості, здійснювати моніторинг і реагування на кіберзагрози, використовувати криптографічні методи та інструменти тестування безпеки;

– формування здатності до самостійного вирішення практичних завдань, ведення документації, роботи в команді та дотримання професійної етики у сфері кібербезпеки.

Основні завдання технологічної практики:

– засвоєння отриманих у процесі навчання теоретичних знань та практичних вмінь і навичок за фахом;

– отримання досвіду входження в трудовий колектив;

– знайомство зі специфікою та напрямками розробки програмного забезпечення на даному конкретному підприємстві, у тому числі з використовуваними на ньому технологіями та засобами розробки;

– отримання інформації про те, які знання, отримані у закладі освіти, і в якому напрямі необхідно поглиблювати і розвивати;

– самостійне виконання здобувачами освіти індивідуальних завдань керівника практики від бази практики;

– формування звітної документації під час та після проходження виробничої практики.

Результати навчання, які дає можливість досягти навчальна дисципліна «Технологічна практика».

РН03. Використовувати результати самостійного пошуку, аналізу та синтезу інформації різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

РН04. Аналізувати, аргументувати, приймати рішення при розв'язанні типових спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН06. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

РН10. Розробляти моделі загроз та порушника.

РН11. Аналізувати проєкти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

РН12. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно- телекомунікаційних системах програмно-апаратними засобами, та давати оцінку якості прийнятих рішень.

РН14. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН15. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

РН19. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

РН20. Брати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

Компетентності, які дає можливість здобути навчальна дисципліна.

Загальні:

ЗК01. Здатність застосовувати знання у практичних ситуаціях.

ЗК04. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК05. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Спеціальні (Фахові):

СК02. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.

СК03. Здатність до розробки та використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК05. Здатність забезпечувати захист інформації, що обробляється В інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК07. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації

СК09. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою.

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

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

Технологічна практика проводиться на підприємствах, в організаціях, науково-дослідницьких та інших установах, що спеціалізуються на наданні послуг в сфері безпеки інформаційних технологій та інших, що мають у складі своєї структури підрозділ з використання сучасних інформаційних та інтелектуальних технологій. Базою проходження технологічної практики студентів спеціальності «Кібербезпека та захист інформації» можуть бути підприємства, організації та установи, діяльність яких пов'язана з інформаційними технологіями, обробкою та захистом даних, а також

забезпеченням кібербезпеки.

До задач, які стоять перед студентами під час проходження виробничої практики, належать:

вивчити:

– організацію і управління діяльністю відповідного підрозділу чи підприємства в цілому;

– технологічні процеси і виробниче обладнання бази практики; діючі

– стандарти, технічні умови, положення та інструкції по експлуатації засобів обчислювальної техніки, вимірювальних приладів та технологічного обладнання, що використовується у виробничій діяльності;

– методи, які застосовуються для вирішення задач науки, техніки, економіки і управління в умовах конкретного підприємства;

– питання організації захисту інформації, забезпечення безпеки життєдіяльності та екологічної чистоти;

– досвід штатних фахівців з інформаційних технологій.

Крім того, кожен студент повинен виконати індивідуальне завдання, зміст якого залежить від особливостей конкретної бази практики. Завдання формулюється керівником практики від бази і затверджується керівником практики від коледжу.

Наведено орієнтовний варіант розподілу кількості днів по етапах проходження технологічної практики в календарному графіку (табл. 1).

Таблиця 1 – Орієнтовний календарний графік проходження практики

№ п/п	Назва етапу	Кількість днів/тижнів
1.	Установча конференція. Основи техніки безпеки та охорони праці	Початок практики
2.	Загальне ознайомлення із структурою підприємства, видом його діяльності та її організацією, методами здійснення управління та контролю.	1 тиждень
3.	Аналіз технічного та програмного забезпечення підприємства.	1 тиждень
4.	Збір, аналіз, систематизація інформації про підприємство для визначення його складових структур та порядку обробки інформації.	1 тиждень
5.	Вивчення складу автоматизованих задач підсистеми, їх	1 тиждень

	інформаційного, програмного, технічного забезпечення	
6.	Проведення інформаційного аналізу та моделювання предметної області підсистеми	2 тиждень
7.	Вивчення інфраструктури корпоративної інформаційної системи підприємства (організації)	2 тиждень
8.	Проаналізувати систему безпеки ІС підприємства(організації) та її відповідність цілям та задачам бізнес-діяльності	2 тиждень
9.	Робота на АРМ спеціаліста функціонального підрозділу чи робочому місці спеціаліста відділу комп'ютеризації та інформаційних технологій	Протягом практики
10.	Виконання індивідуального завдання	Протягом практики
11.	Оформлення звіту.	Протягом практики

Таблиця 2 – Тематичний план

№ п/п	Назва теми	Кількість годин
1.	Ознайомлення з підприємством. Інструктаж з протипожежного захисту об'єкту та технікою безпеки на підприємстві.	12
2.	Вивчення основних функцій організації, оснащення організації апаратним та програмним забезпеченням, їх особливостями.	6
3.	Вивчення специфіки роботи підприємства	6
4.	Ознайомлення з роботою спеціаліста з інформаційної безпеки. Короткий опис посадових обов'язків	18
5.	Аналіз технічного та програмного забезпечення діяльності підприємства	12
6.	Опис існуючої безпекової моделі підприємства	18
7.	Визначення предметної області та проблеми підприємства	6
8.	Аналіз вимог до впроваджуваного рішення	18
9.	Створення технічного завдання до програмного продукту	18
10.	Проєктування системи захисту	36
11.	Розробка моделі загроз і сценарії атак	6
12.	Робота на штатних робочих місцях	96
13.	Формування очікуваних результатів проєктованого рішення	6
14.	Систематизація матеріалів, оформлення звітів, отримання виробничої характеристики і залік з виробничої практики.	12
	Всього:	**270**

2.3 Виробнича практика

Виробнича практика для здобувачів освіти спеціальності 125 «Кібербезпека та захист інформації» проводиться на IV курсі у 8 семестрі. Тривалість виробничої практики – шість тижнів, кількість кредитів – 9 (270 годин), форма підсумкового контролю – залік (захист звітів по практиці).

Виробнича практика ставить за мету:

– оволодіти сучасними методами, формами організації праці у галузі майбутньої професії;

– набути професійних умінь і навичок, необхідних для прийняття самостійних рішень;

– закріпити і поглибити знання здобуті при вивченні спеціальних дисциплін, навчитися застосовувати їх у професійній діяльності;

– набути практичних навичок і досвіду аналізу предметних областей та їх формалізації при проєктуванні моделі інформаційної безпеки;

– сформувати професійні вміння і навички у роботі з існуючими інформаційними технологіями;

– виховання потреби систематичного оновлення своїх знань та їх творчого застосування у практичній діяльності;

– ознайомитись безпосередньо на підприємствах, в організаціях, установах з підготовкою до виробничого процесу, закріпити знання та вміння, здобуті при опануванні певного циклу теоретичних дисциплін, а також придбати певний практичний досвід.

Основні завдання практики:

– закріпити і поглибити теоретичні знання шляхом вивчення досвіду діяльності підприємства, придбати досвід практичної роботи на підприємствах, перевірити рівень професійної підготовки та ділових якостей студентів;

– вивчити і опанувати функціональні обов'язки, службових осіб з майбутньої спеціальності та отримати професійні знання, уміння, навички при виконанні конкретних практичних завдань на штатних посадах або на посадах дублерів.

– вивчити специфіку предметної області конкретного об'єкта управління та

провести її аналіз;

– вивчити досвід організації інформаційних технологій на підприємстві, автоматизувати роботу однієї з ланок підприємств, організацій різних форм власності та установ;

– ознайомитись зі складом та характеристиками комп'ютерного парку, що застосовується, його розміщенням та засобами зв'язку, вивчити топологію комп'ютерної мережі;

– ознайомитись зі складом та характеристиками існуючого загальносистемного програмного забезпечення;

– протестувати спроєктовану модель інформаційної безпеки, в комплексі існуючих рішень підприємства.

Після проходження виробничої практики студенти повинні вміти:

– організовувати основні факти, концепції, принципи та технології проєктування та створення систем, порядок їх документального оформлення, порядок проведення робіт зі створення систем;

– виконувати на професійному рівні пошук матеріалів з фахових питань за допомогою сучасної науково-технічної, довідкової літератури, інформаційно-довідкових систем з використанням комп'ютеризованих систем опрацювання та пошуку інформації;

– планувати власну діяльність з використанням теорії прийняття рішень у професійній діяльності, комп'ютерних систем забезпечення прийняття рішень;

– узгоджувати рішення, що приймаються, з нормативними актами галузі та чинним законодавством;

– створювати соціально-економічні відносини між членами трудового колективу на правових засадах і демократичних принципах;

– орієнтуватися у державних та міжнародних стандартах (І8О/ІЕС,НД ТЗІ, рекомендаціях М8Т тощо);

– визначати відповідність політик підприємства вимогам нормативних документів;

– використовувати сучасні ІКТ, методи, моделі та засоби захисту інформації в інформаційно-телекомунікаційних системах;

– працювати з програмними та програмно-апаратними засобами безпеки;

– проводити моніторинг інформаційних потоків та подій безпеки згідно з політикою підприємства;

– виявляти відхилення, потенційні інциденти, порушення політик доступу;

– адаптуватися до нових технологій та інструментів, оперативно реагувати на технологічні зміни;

– виконувати тестування засобів захисту та оцінювання їх ефективності.

Результати навчання, які дає можливість досягти навчальна дисципліна.

РН03. Використовувати результати самостійного пошуку, аналізу та синтезу інформації різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

РН04. Аналізувати, аргументувати, приймати рішення при розв'язанні типових спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН06. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

РН10. Розробляти моделі загроз та порушника.

РН11. Аналізувати проєкти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

РН12. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно- телекомунікаційних системах програмно-апаратними засобами, та давати оцінку якості прийнятих рішень.

РН13. Реалізовувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативно-правових документів.

РН14. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН15. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

РН16. Забезпечувати функціонування спеціального програмного забезпечення,

щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

РН17. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і або кібербезпеки.

Компетентності, які дає можливість здобути навчальна дисципліна.

Загальні:

ЗК01. Здатність застосовувати знання у практичних ситуаціях.

ЗК04. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК05. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК08. Здатність працювати в команді.

Спеціальні (Фахові):

СК02. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.

СК03. Здатність до розробки та використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК04. Здатність забезпечувати працездатність в інформаційно-комунікаційних систем згідно зі встановленою політикою безпеки.

СК05. Здатність забезпечувати захист інформації, що обробляється В інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК07. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації

СК09. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою.

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

СК11. Здатність виконувати моніторинг процесів функціонування

інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

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

Результатом проходження практики є здобуття практичного досвіду забезпечення інформаційної безпеки, формування навичок роботи з реальними інфраструктурами, розвиток здатності оперативно реагувати на інциденти та готовність до виконання професійних обов'язків з кібербезпеки та захисту інформації.

Виробнича практика проводиться на підприємствах, в організаціях, науково-дослідницьких та інших установах, що спеціалізуються на наданні послуг в сфері інформаційних технологій та інших, що мають у складі своєї структури підрозділ з використання сучасних інформаційних та інтелектуальних технологій.

Підприємства, які можуть бути базою практики для студентів спеціальності «Кібербезпека та захист інформації», повинні відповідати низці професійних та організаційних вимог. Насамперед це має бути офіційно зареєстрований суб'єкт господарювання, діяльність якого пов'язана з інформаційними технологіями, захистом інформації, телекомунікаціями або експлуатацією інформаційних систем. Важливо, щоб профіль діяльності підприємства забезпечував можливість здобуття практичних навичок у сфері кібербезпеки, зокрема в адмініструванні мереж і систем, аналізі вразливостей, тестуванні на проникнення, криптографічному захисті інформації чи аудиті інформаційної безпеки.

Підприємство повинно мати належну матеріально-технічну базу, яка включає сучасну комп'ютерну техніку, спеціалізоване програмне забезпечення, мережеве обладнання та, за можливості, системи моніторингу безпеки. Не менш важливою є наявність кваліфікованих фахівців, здатних здійснювати керівництво практикою студентів, надавати консультації та контролювати виконання поставлених завдань. Організаційно підприємство забезпечує призначення керівника практики, погодження індивідуального плану роботи студента, а також створення умов для його залучення до реальних або наближених до реальних професійних завдань.

До задач, які стоять перед здобувачами освіти під час проходження виробничої практики, належать:

- закріплення та поглиблення теоретичних знань, отриманих у процесі навчання;
- набуття практичних умінь і навичок у сфері кібербезпеки;
- ознайомлення зі структурою підприємства та організацією роботи IT-підрозділів і служб інформаційної безпеки;
- вивчення нормативної, технічної та внутрішньої документації підприємства;
- застосування сучасних методів і засобів захисту інформації;
- виконання базового адміністрування комп'ютерних систем і мереж;
- здійснення моніторингу подій інформаційної безпеки;
- виявлення, аналіз та оцінювання потенційних загроз і вразливостей;
- участь у впровадженні та налаштуванні засобів кіберзахисту;
- виконання елементарного аудиту інформаційної безпеки;
- оцінювання ризиків для інформаційних систем і ресурсів;
- підготовка звітів за результатами виконаних завдань;
- формування рекомендацій щодо підвищення рівня захищеності систем;
- розвиток навичок самостійної роботи та прийняття рішень;
- формування вміння працювати в команді;
- дотримання вимог професійної етики та конфіденційності інформації.

Орієнтовна програма виробничої практики наведена в таблиці 1.

Наведено орієнтовний варіант розподілу кількості днів по етапах проходження виробничої практики в календарному графіку (табл. 1).

Таблиця 1 – Орієнтовний календарний графік проходження практики

№ п/п	Назва етапу	Кількість днів/тижнів
1.	Оформлення на базі практики, проходження інструктажів з техніки безпеки та інформаційної безпеки	1 тиждень
2.	Загальне ознайомлення із структурою підприємства, видом його діяльності та її організацією, методами здійснення управління та контролю	1 тиждень
3.	Вивчення внутрішніх регламентів, політик безпеки та документації	1 тиждень

4.	Збір, аналіз, систематизація інформації про підприємство для визначення його складових структур та порядку обробки інформації	1 тиждень
5.	Вивчення складу автоматизованих задач підсистеми, їх інформаційного, програмного, технічного забезпечення	1 тиждень
6.	Виконання завдань з адміністрування комп'ютерних систем і мереж	2 тиждень
7.	Робота з користувачами, налаштування робочих місць, ознайомлення з програмними та апаратними засобами захисту інформації	2 тиждень
8.	Проаналізувати систему безпеки підприємства (організації) та її відповідність цілям та задачам бізнес-діяльності, участь у моніторингу подій безпеки.	2,3 тиждень
9.	Аналіз вразливостей інформаційних систем	2,3 тиждень
10.	Участь у тестуванні безпеки	4,5 тиждень
11.	Робота з системами захисту (антивірус, фаєрволи, IDS/IPS)	3,4,5 тиждень
12.	Виконання індивідуального завдання	Протягом практики
13.	Оформлення результатів виконаних робіт; підготовка звіту з практики; узгодження матеріалів із керівником від підприємства; отримання відгуку та характеристики; захист практики у закладі освіти.	6 тиждень

Таблиця 2 – Тематичний план

№ п/п	Назва теми	Кількість годин
1.	Вступ до практики. Ознайомлення з підприємством, інструктаж з охорони праці та інформаційної безпеки.	6
2.	Організаційна структура IT-підрозділу та служби інформаційної безпеки.	6
3.	Нормативно-правове забезпечення та політики інформаційної безпеки на підприємстві.	6
4.	Апаратне та програмне забезпечення інформаційних систем.	24
5.	Основи адміністрування комп'ютерних систем і мереж.	12
6.	Налаштування та обслуговування робочих станцій користувачів.	18
7.	Мережеві технології та протоколи, їх захист.	24
8.	Засоби захисту інформації: антивірусні системи, міжмережеві екрани, системи виявлення вторгнень.	12
9.	Моніторинг подій інформаційної безпеки та реагування на інциденти.	18
10.	Аналіз загроз і вразливостей інформаційних систем.	18
11.	Основи тестування на проникнення (pentesting).	6
12.	Криптографічний захист інформації та управління доступом.	18

13.	Резервне копіювання та відновлення даних.	12
14.	Аудит інформаційної безпеки та оцінювання ризиків.	18
15.	Документування процесів і підготовка технічної звітності.	12
16.	Виконання індивідуального завдання за тематикою практики.	48
17.	Оформлення звіту з практики, узагальнення отриманих на виробництві матеріалів	12
	Всього:	**270**

Індивідуальне завдання надається безпосередньо на підприємстві керівником від бази практики і узгоджується з керівником від циклової комісії. Завдання може бути також учбовим, але наближеним до тематики, якою займається підприємство.

Орієнтовні теми індивідуальних завдань для виробничої практики студентів спеціальності «Кібербезпека та захист інформації» наведено нижче.

1) Аналіз системи інформаційної безпеки підприємства та розробка рекомендацій щодо її вдосконалення.

2) Оцінювання вразливостей локальної мережі та підготовка звіту з пропозиціями щодо їх усунення.

3) Налаштування та аналіз ефективності міжмережевого екрана (Firewall).

4) Дослідження роботи антивірусного програмного забезпечення та політик захисту.

5) Проведення базового тестування на проникнення вебресурсу.

6) Аналіз та налаштування системи виявлення вторгнень.

7) Розробка політики паролів та управління доступом на підприємстві.

8) Організація резервного копіювання та відновлення даних.

9) Дослідження методів захисту бездротових мереж (Wi-Fi).

10) Аналіз журналів подій безпеки та виявлення інцидентів.

11) Оцінювання ризиків інформаційної безпеки для підприємства.

12) Розробка моделі загроз для інформаційної системи.

13) Дослідження криптографічних методів захисту даних у корпоративних системах.

14) Аналіз безпеки вебдодатків.

15) Розробка рекомендацій щодо захисту персональних даних відповідно до нормативних вимог.

16) Автоматизація процесів моніторингу безпеки з використанням скриптів.

17) Налаштування системи контролю доступу в операційних системах.

18) Аналіз безпеки хмарних сервісів, що використовуються підприємством.

19) Розробка інструкції з інформаційної безпеки для працівників.

20) Аналіз інцидентів кібербезпеки та розробка плану реагування.

21) Порівняльний аналіз сучасних засобів захисту інформації.

22) Створення тестового середовища для дослідження кіберзагроз.

Для кожного завдання студент повинен підготувати детальний опис його виконання, який так само подається у звіті про виконання програми практики та оцінюється керівниками практики під час захисту практики. У результаті виконання завдання готується детальний опис потоків інформації з переліком супроводжувальної документації від вхідної до вихідної та переліком методів збору та опрацювання інформації на підприємстві.