МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

Кафедра кібербезпеки та інформаційних технологій

«ЗАТВЕРДЖУЮ»
Проректор з навчально-методичної роботи
_____

НАСКРІЗНА ПРОГРАМА ПРАКТИКИ

рівень вищої освіти перший (бакалаврський)
галузь знань 12 «Інформаційні технології»
спеціальність 125 «Кібербезпека»
освітньо-професійна програма «Кібербезпека»

Завідувачка кафедри кібербезпеки та інформаційних технологій
_____ Старкова О. В.
(підпис) (прізвище та ініціали)

Гарант освітньо-професійної програми Кібербезпека
_____ Лимаренко В. В.
(підпис) (прізвище та ініціали)

Укладачі: _____ Старкова О. В.
(підпис) (прізвище та ініціали)
_____ Лимаренко В. В.
(підпис) (прізвище та ініціали)

Харків
ХНЕУ ім. С. Кузнеця
2023

УДК 004.056(076.034)
Н31

Укладачі: О. В. Старкова
В. В. Лимаренко

Затверджено на засіданні кафедри кібербезпеки та інформаційних технологій.
Протокол № 8 від 24.12.2022 р.

Самостійне електронне текстове мережеве видання

Наскрізна програма практики для студентів спеціальності
Н31 125 "Кібербезпека" освітньої програми "Кібербезпека" першого (бакалаврського) рівня [Електронний ресурс] / уклад. О. В. Старкова, В. В. Лимаренко. – Харків : ХНЕУ ім. С. Кузнеця, 2023 – 26 с.

Подано загальні положення, мету та завдання, зміст і структуру навчальної, виробничої та переддипломної практики. Описано процес організації, принципи керівництва та контролю проходження практик за видами. Визначено порядок звітності за результатами практик, їхній захист і підсумковий контроль.

Рекомендовано для студентів спеціальності 125 "Кібербезпека" освітньої програми "Кібербезпека" першого (бакалаврського) рівня.

УДК 004.056(076.034)

Вступ

Наскрізну програму практики складено відповідно до Положення про проведення практики студентів Харківського національного економічного університету імені Семена Кузнеця, розробленого, згідно із Законом України "Про вищу освіту", Положенням про проведення практики студентів вищих навчальних закладів України, затвердженого наказом Міністерства освіти і науки України від 08.04.1993 р. № 93, Положенням про організацію освітнього процесу в Харківському національному економічному університеті імені Семена Кузнеця, уведеного в дію наказом університету від 26.10.2020 р. № 198, стандартами вищої освіти, освітньо-професійною програмою Кібербезпека, першого (бакалаврського) рівня спеціальності 125 "Кібербезпека".

Програма практичної підготовки дозволяє здобувачам вищої освіти скласти чітке уявлення про те, що їм доведеться виконувати під час практики, як вирішити індивідуальне завдання, яку допомогу вони можуть дістати від керівників практики, закладу вищої освіти та підприємства (організації, установи), а також працівників (керівників) підприємства, із якими вони будуть зустрічатися під час практики.

Здобувачі вищої освіти дістануть необхідний обсяг практичних знань і умінь, відповідно до складених робочих програм практик.

1. Види, загальні характеристики, мета та заплановані результати практик

1.1. Види практик (табл. 1):

Таблиця 1

Види практик

Курси	Назви практик	Очна (денна) форма навчання	Кафедри, що забезпечують організацію	Тривалість практики	Семестри
III	Виробнича	+	кібербезпеки та інформаційних технологій	Два тижні	6-й
IV	Переддипломна	+	кібербезпеки та інформаційних технологій	Два тижні	8-й

1.2. Характеристика практик (табл. 2).

Усі види практик є обов'язковими освітніми компонентами.

Таблиця 2

Характеристика практик

Курси	Назви практик	Очна (денна) форма навчання	Кількість кредитів	Загальна кількість годин	Семестри	Форми контролю
III	Виробнича	+	3	90	6-й	Звіт
IV	Переддипломна	+	2	60	8-й	Звіт

1.3. Мета практик.

1.3.1. Виробнича практика.

Виробнича практика є частиною навчального процесу й організовується для студентів третього курсу денної форми навчання першого

(бакалаврського) рівня вищої освіти за спеціальністю "Кібербезпека та захист інформації" у шостому семестрі.

Мета практики – забезпечення єдності теоретичного та практичного навчання студентів із питань використання методів аналізу протидії сучасним гібридним атакам, оцінювання поточного рівня безпеки та вибору механізмів протидії під час дослідження стану предметної області на базі практики, аналізу інфраструктури мережі, технічних засобів комплексної системи захисту інформації, можливості її удосконалення в умовах дії сучасних кіберзагроз.

Завданнями практики є:

1. Закріплення, поглиблення та доповнення теоретичних знань, які набуваються під час засвоєння курсів циклу природничо-наукової підготовки і циклу професійної та практичної підготовки.

2. Підготовка до вивчення профільних дисциплін.

3. Збір матеріалів для виконання курсових проектів.

Під час проходження практики необхідно зібрати матеріал у межах поставленого керівником завдання та виконати таке:

1. Навести схему організаційної структури підприємства із зазначенням того, які інформаційні ресурси обробляються в мережі, які технічні засобі та програмні застосунки забезпечення безпеки даних використовуються на підприємстві. Окремо вказати місце підрозділу, де безпосередньо буде проходити практика, склад посадових осіб конкретного підрозділу та їхні функції, інформаційні зв'язки цього підрозділу з ближнім оточенням.

2. Навести опис складу та структури наявної інформаційної системи на об'єкті: характеристика інформаційного та програмного забезпечення, яке забезпечує безпеку даних у мережі, склад функціональних підсистем. Детально описати функціональну підсистему, на якій виконувалося особисте завдання.

3. Подати опис наявних засобів виявлення аномалій у нормальній роботі системи та організацію виконання профілів безпеки. Провести аналіз можливих загроз на конфіденційну (комерційну) інформацію.

4. Під час виконання особистого завдання, виданого викладачем, слід розробити глосарій проекту (перелічити спеціальні терміни та їх значення), структурну схему локальної (корпоративної мережі) із зазначенням програмних (програмно-апаратних) засобів забезпечення безпеки.

5. Навести обґрунтування необхідності та можливості удосконалення або встановлення додаткових програмних застосунків щодо підвищення рівня безпеки в локальної/корпоративній мережі організації.

1.3.2. Переддипломна практика.

Метою переддипломної практики є узагальнення, систематизація, закріплення та поглиблення теоретичних знань студентів за профільними дисциплінами, що вивчені за спеціальністю "Кібербезпека та захист інформації", отримання навичок проведення аналізу сучасної системи захисту конкретного об'єкта з метою самостійного моделювання можливих кіберзагроз та розроблення плану кіберзахисту інформаційної системи.

Завдання переддипломної практики:

1. Зібрати матеріал за темою дипломного проєкту для оцінювання стану системи захисту об'єкта управління.

2. Вивчити на практиці сучасні методи реалізації несанкціонованого доступу та захисту інформації від стороннього впливу.

3. Вивчити специфіку інформаційного потоку конкретного об'єкта управління, що підлягає захисту.

4. Розробити вимоги щодо захисту інформації об'єкта управління від несанкціонованого доступу.

5. Проаналізувати сучасні наявні засоби захисту інформації в інформаційно-комунікаційних системах від витоку її технічними каналами.

6. Розробити вимоги щодо використання засобів захисту інформації в інформаційно-комунікаційних системах від витоку її технічними каналами за межі об'єкта управління.

1.4. Заплановані компетентності та результати навчання (табл. 3).

Таблиця 3

Заплановані компетентності та результати навчання

Спеціальні компетентності	Загальні компетентності	Результати навчання
1	2	3
Виробнича практика		
–	КЗ 1, КЗ 2, КЗ 3	РН 1
–	КЗ 1, КЗ 2, КЗ 4, КЗ 5	РН 2

Продовження табл. 3

1	2	3
–	КЗ 1, КЗ 2, КЗ 4, КЗ 5	РН 3
–	КЗ 1, КЗ 2, КЗ 4, КЗ 5	РН 4
–	КЗ 2, КЗ 4, КЗ 5	РН 5
КФ 1	КЗ 2, КЗ 4	РН 7
КФ 1	КЗ 2, КЗ 4	РН 8
КФ 2, КФ 11	КЗ 1	РН 10
КФ 2, КФ 11	КЗ 1	РН 11
КФ 2, КФ 3, КФ 5, КФ 11	КЗ 1	РН 18
КФ 2, КФ 5, КФ 8, КФ 11	КЗ 1	РН 19
КФ 2, КФ 3, КФ 5, КФ 6, КФ 10	КЗ 1	РН 20
КФ 5, КФ 9, КФ 11	КЗ 1	РН 21
КФ 5, КФ 11	КЗ 1	РН 22
КФ 4, КФ 5, КФ 9, КФ 11	КЗ 1	РН 24
КФ 4, КФ 5, КФ 6	КЗ 1	РН 27
КФ 4, КФ 5, КФ 8, КФ 11	КЗ 1	РН 32
КФ 1, КФ 3, КФ 4, КФ 5, КФ 7, КФ 8, КФ 9, КФ 12	КЗ 1	РН 35
КФ 2, КФ 3, КФ 4, КФ 5, КФ 6, КФ 8, КФ 11, КФ 12	КЗ 1, КЗ 4	РН 53
–	КЗ 1, КЗ 2, КЗ 6, КЗ 7	РН 54
Переддипломна практика		
–	КЗ 1, КЗ 2, КЗ 3	РН 1
–	КЗ 1, КЗ 2, КЗ 4, КЗ 5	РН 2
–	КЗ 1, КЗ 2, КЗ 4, КЗ 5	РН 3
–	КЗ 1, КЗ 2, КЗ 4, КЗ 5	РН 4
–	КЗ 2, КЗ 4, КЗ 5	РН 5
–	КЗ 2	РН 6
КФ 1	КЗ 2, КЗ 4	РН 7
КФ 1	КЗ 2, КЗ 4	РН 8
КФ 1, КФ 3, КФ 4, КФ 5, КФ 7, КФ 8, КФ 9, КФ 11, КФ 12	КЗ 5	РН 9
КФ 2, КФ 11	КЗ 1	РН 10
КФ 2, КФ 5, КФ 8, КФ 11, КФ 12	КЗ 5	РН 13
КФ 2, КФ 3, КФ 5, КФ 8, КФ 10, КФ 11	–	РН 14
КФ 2, КФ 3, КФ 4, КФ 5, КФ 6, КФ 8, КФ 11	КЗ 2	РН 17

Закінчення табл. 3

1	2	3
КФ 2, КФ 3, КФ 5, КФ 11	КЗ 1	РН 18
КФ 2, КФ 5, КФ 8, КФ 11	КЗ 1	РН 19
КФ 2, КФ 3, КФ 5, КФ 6, КФ 10	КЗ 1	РН 20
КФ 5, КФ 9, КФ 11	КЗ 1	РН 21
КФ 5, КФ 11	КЗ 1	РН 22
КФ 4, КФ 5, КФ 9, КФ 11	КЗ 1	РН 24
КФ 4, КФ 5, КФ 6	КЗ 1	РН 27
КФ 5, КФ 9, КФ 12	КЗ 5	РН 28
КФ 2, КФ 6, КФ 10	–	РН 31
КФ 4, КФ 5, КФ 8, КФ 11	КЗ 1	РН 32
КФ 1, КФ 3, КФ 4, КФ 5, КФ 7, КФ 8, КФ 9, КФ 12	КЗ 1	РН 35
КФ 10	–	РН 36
КФ 6, КФ 10	–	РН 37
КФ 6, КФ 10	–	РН 38
КФ 10	–	РН 39
КФ 10	–	РН 40
КФ 8, КФ 11	–	РН 41
КФ 1, КФ 4, КФ 5, КФ 8, КФ 9, КФ 11, КФ 12	КЗ 2	РН 43
КФ 2, КФ 3, КФ 5, КФ 10	–	РН 47
КФ 5, КФ 6, КФ 8, КФ 10, КФ 11	–	РН 48
КФ 2, КФ 3, КФ 4, КФ 5, КФ 6, КФ 8, КФ 11, КФ 12	КЗ 1, КЗ 4	РН 53
–	КЗ 1, КЗ 2, КЗ 6, КЗ 7	РН 54

Примітка.

КФ 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 безпеки та/або кібербезпеки.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

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

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної безпеки та/або кібербезпеки.

КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою.

КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно із встановленою політикою інформаційної безпеки та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості та дестабілізувальні чинники інформаційному простору та інформаційним ресурсам згідно із встановленою політикою інформаційної безпеки та/або кібербезпеки.

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області й розуміння професії.

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

КЗ 4. Уміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КЗ 6. Здатність реалізувати свої права й обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини та громадянина в Україні.

КЗ 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.

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

РН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи вирішення складних спеціалізованих завдань та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного вирішення спеціалізованих завдань професійної діяльності.

РН 4. Аналізувати, аргументувати, ухвалювати рішення під час вирішення складних спеціалізованих завдань та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за ухвалені рішення.

РН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

РН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, зокрема міжнародних у галузі інформаційної безпеки та/або кібербезпеки.

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

РН 9. Впроваджувати процеси, що базуються на національних і міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки та/або кібербезпеки.

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

РН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

РН 13. Аналізувати проєкти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості ухвалених рішень.

РН 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 і моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

РН 20. Забезпечувати функціонування спеціального програмного забезпечення щодо захисту інформації від руйнувальних програмних впливів і кодів у інформаційно-телекомунікаційних системах.

РН 21. Вирішувати завдання забезпечення та супроводу (зокрема: огляд, тестування, підзвітність) системи управління доступом згідно із встановленою політикою безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

РН 22. Вирішувати завдання управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів у інформаційно-телекомунікаційних системах згідно із встановленою політикою інформаційної безпеки та/або кібербезпеки.

РН 24. Вирішувати завдання управління доступом до інформаційних ресурсів і процесів у інформаційних і інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

РН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

РН 28. Аналізувати та проводити оцінювання ефективності та рівня захищеності ресурсів різних класів у інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах у ході проведення випробувань згідно із встановленою політикою інформаційної безпеки та/або кібербезпеки.

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

РН 32. Вирішувати завдання управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно із встановленою політикою безпеки.

РН 35. Вирішувати завдання забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів у інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно із встановленою політикою інформаційної безпеки та/або кібербезпеки.

РН 36. Виявляти небезпечні сигнали технічних засобів.

РН 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.

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

РН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

РН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

РН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

РН 43. Застосовувати національні та міжнародні регулювальні акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.

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

РН 48. Виконувати впровадження та підтримку систем виявлення вторгнень і використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

РН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

РН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в України.

2. Зміст практик

2.1. Виробнича практика.

Зміст виробничої практики визначається її керівником на основі робочої програми та відображається в індивідуальному плані студента.

Студент під час проходження виробничої практики зобов'язаний:

1) повністю виконати завдання, передбачені програмою практики, включно з індивідуальним завданням;

2) виконувати чинні на підприємстві правила внутрішнього розпорядку;

3) пройти інструктаж і суворо дотримуватися правил охорони праці, техніки безпеки та виробничої санітарії;

4) виконувати та нести відповідальність за виконану роботу на підприємстві за дорученням керівника практики нарівні зі штатними співробітниками;

5) вести щоденник практики за етапами її проходження;

6) подати на кафедру письмовий звіт про виконання виробничої практики та індивідуального завдання разом із відгуком, підписаним керівником (куратором) практики від підприємства;

7) захистити основні положення, відображені у звіті.

2.2. Переддипломна практика.

Зміст переддипломної практики визначається її керівником на основі робочої програми, теми дипломного проєкту та відображається в індивідуальному плані студента.

Студент під час проходження переддипломної практики зобов'язаний:

1) повністю виконати завдання, передбачені програмою практики, з урахуванням індивідуального завдання;

2) виконувати чинні на підприємстві правила внутрішнього розпорядку;

3) пройти інструктаж і суворо дотримуватися правил охорони праці, техніки безпеки та виробничої санітарії;

4) виконувати та нести відповідальність за виконану роботу на підприємстві за дорученням керівника практики нарівні зі штатними співробітниками;

5) вести щоденник практики за етапами її проходження;

6) подати на кафедру письмовий звіт про виконання переддипломної практики та індивідуального завдання разом із відгуком, підписаним керівником (куратором) практики від підприємства;

7) захистити основні положення, відображені у звіті.

У процесі переддипломної практики студенти мають виконати такі завдання:

1) описати напрямки діяльності об'єкта управління;

2) проаналізувати стан системи безпеки об'єкта управління;

3) проаналізувати наявні методи реалізації несанкціонованого доступу, які можуть бути застосованими для об'єкта управління;

4) проаналізувати наявні методи захисту інформації від несанкціонованого доступу;

5) розробити вимоги щодо захисту інформації від несанкціонованого доступу;

6) проаналізувати технічні канали інформаційно-комунікаційної системи об'єкта управління;

7) запропонувати необхідні засоби захисту інформації в інформаційно-комунікаційних системах від витоку її технічними каналами.

3. Вимоги до баз практик

3.1. Виробнича та переддипломна практика.

Виробнича та переддипломна практики проводяться на підприємствах, в організаціях, науково-дослідницьких та інших установах, що спеціалізуються на наданні послуг у сфері інформаційних технологій та інформаційної безпеки, банках, страхових компаніях, компаніях-операторах зв'язку та інших, що мають у складі своєї структури підрозділ, що відповідає за інформаційну безпеку, або в будь-яких організаціях, де використовуються технічні засоби оброблення, зберігання та передачі конфіденційної інформації.

Закріплення баз практики має сприяти встановленню та зміцненню довгострокових контактів університету з підприємствами, а також розвитку кооперації між ними з метою якісної підготовки фахівців. Визначенню баз практик має передувати постійна робота кафедри щодо вивчення виробничих та економічних можливостей підприємств з погляду їхньої придатності для проведення практики студентів за спеціальністю. До цього ж мають враховуватися перспективи сучасних напрямів розвитку ІТ-галузі, економічного, соціального та екологічного розвитку суспільства.

До підприємств – баз виробничої та переддипломної практики висуваються такі вимоги:

здійснення діяльності дослідження, проєктування, розроблення, впровадження й експлуатації програмних засобів;

наявність високого рівня технічного забезпечення, використання сучасних інформаційних та інтелектуальних технологій;

забезпечення проходження практики невеликими групами студентів.

Бази практики повинні: мати високий рівень технічного забезпечення, використовувати сучасну обчислювальну техніку та інформаційні технології; забезпечувати можливість проведення виробничої та переддипломної практики з дотриманням програми; мати науково-технічні зв'язки з закладом вищої освіти (ЗВО).

4. Організація проведення та керівництво практиками

4.1. Виробнича практика.

Виробнича практика може проводитися в державних, муніципальних, громадських, комерційних і некомерційних організаціях чи підприємствах,

де можливий збір і вивчення матеріалів, що пов'язані з аналізом стану безпеки інформаційних ресурсів, а також у навчальних та наукових підрозділах університету за напрямом підготовки студентів.

Організація практики на всіх етапах спрямована на забезпечення безперервності і послідовності оволодіння студентами навичками та вміннями професійної діяльності відповідно до вимог згідно з рівнем підготовки бакалавра. Практика проводиться відповідно до індивідуальної програми виробничої практики, що узгоджена студентом та науковим керівником на основі загальних підходів до її змісту та структури.

Перед початком практики проводяться консультаційні збори, на яких надається вся необхідна інформація з порядку проведення виробничої практики та консультація з техніки безпеки. За результатами зборів студенти заповнюють щоденники, в яких наводять: відомості про себе, назву бази практики, вид практики, період проходження практики, календарний графік із переліком запланованих до виконання робіт. Календарний графік студенти завіряють підписом керівника від університету, підписом декану факультету та печаткою факультету. За необхідності студентом на базу практики надається направлення від університету.

На першому тижні практики студент має:

отримати завдання для проходження виробничої практики;

узгодити графік консультацій зі своїм керівником на кафедрі та ознайомитися з графіком відвідувань цієї бази практики уповноваженими викладачами-консультантами;

завірити підписом календарний графік у завідувача кафедри "Кібербезпеки та інформаційних технологій" або уповноваженою ним особою (для тих, хто проходить практику на кафедрі), або у керівника іншої бази практики (для тих, хто проходить практику за межами університету);

завірити підписом та печаткою керівництва бази практики прибуття студента на практику;

пройти інструктаж із техніки безпеки на базі практики.

На останньому тижні практики студент має:

після закінчення терміну проходження практики за результатами виконаних робіт оформити робочі записи у щоденнику й отримати відгуки керівника від кафедри та керівника від бази практики;

завірити підписом і печаткою керівництва бази практики вибуття студента із практики;

сформувати звіт, титульний аркуш якого підписати з боку студента, керівника від університету та керівника від бази практики;

якщо базою практики не є університет, то на підпис керівника від бази практики поставити печатку підприємства.

Індивідуальний план виробничої практики студента має бути узгоджений з планом роботи організації, що є базою практики. У період практики студенти підкоряються всім правилам внутрішнього розпорядку і техніки безпеки, встановленим у підрозділі та на робочих місцях.

Після закінчення практики студенти оформляють всю необхідну документацію відповідно до вимог програми виробничої практики.

Загальне методичне керівництво практикою здійснюється випускаючим структурним підрозділом – кафедрою "Кібербезпеки та інформаційних технологій". Загальне керівництво виробничою практикою здійснює науковий керівник від кафедри. Для проходження практики для всіх студентів визначаються куратори від бази практики, під керівництвом яких студенти виконують поставлені в програмі завдання. Керівник виробничої практики від кафедри надає студенту організаційне сприяння та методичну допомогу у вирішенні завдань.

Керівник практики від кафедри:

1) погоджує програму виробничої практики і тему завдання з науковим керівником;

2) надає консультації студентам за попередньо узгодженим графіком і проводить перевірку проходження практики студентами та надає їм консультації на тих базах практики, які зазначені;

3) встановлює зв'язок із керівниками практики від організації та спільно з ними складає робочу програму проведення практики;

4) розробляє тематику індивідуальних завдань;

5) сприяє формуванню загальної схеми виконання завдання, графіка проведення практики, режиму роботи студентів і здійснює систематичний контроль ходу практики та роботою студентів;

6) бере участь у розподілі студентів за робочими місцями або переміщення їх за видами робіт;

7) несе відповідальність разом із керівником практики від організації за дотримання студентами правил техніки безпеки;

8) здійснює контроль дотримання термінів практики та її змісту;

9) надає методичну допомогу студентам під час виконання ними індивідуальних завдань і збору матеріалів для курсової роботи;

10) оцінює результати виконання студентами програми практики та вносить їх як у вигляді оцінки, так і у вигляді відгуку за результатами роботи студента.

Керівник практики від бази практики:

1) погоджує програму виробничої практики згідно зі встановленою темою завдання;

2) надає консультації студентам щодо організації збору необхідної інформації за темою завдання;

3) встановлює зв'язок із керівниками практики від університету;

4) розробляє тематику індивідуальних завдань;

5) сприяє виконанню режиму роботи студентів і здійснює систематичний контроль проведення практики та роботи студентів;

6) бере участь у розподілі студентів за робочими місцями або переміщення їх за видами робіт;

7) несе відповідальність разом із керівником практики від університету за дотримання студентами правил техніки безпеки;

8) здійснює контроль дотримання термінів практики та її змісту;

9) оцінює результати виконання студентами програми практики та вносить їх як у вигляді оцінки, так і у вигляді відгуку за результатами роботи студента у щоденник з практики.

Науковий керівник студента:

1) координує постановку завдань із самостійної роботи студентів у період практики за виданим індивідуальним завданням зі збору необхідних матеріалів, надає відповідну консультаційну допомогу;

2) дає рекомендації щодо вивчення спеціальної літератури;

3) бере участь у роботі конференції з ведення підсумків виробничої практики.

Студент під час проходження практики отримує від керівника практики, а також від свого наукового керівника вказівки, рекомендації та роз'яснення з усіх питань, пов'язаних з організацією та проходженням практики, звітує про виконання робіт відповідно до графіка проведення практики.

Студент:

1) проводить збір матеріалів за обраним завданням відповідно до графіка практики та режимом роботи підрозділу – місця проходження практики;

2) отримує від керівника практики вказівки, рекомендації та роз'яснення з усіх питань, пов'язаних з організацією та проходженням практики;

3) звітує про виконану роботу відповідно до встановленого графіка.

4.2. Переддипломна практика.

Переддипломна практика може проводитися в державних, муніципальних, громадських, комерційних і некомерційних організаціях чи підприємствах, де можливий збір і вивчення матеріалів, пов'язаних із виконанням сучасних бізнес-процесів, а також у навчальних та наукових підрозділах університету за напрямом підготовки студентів.

Організацію практики на всіх етапах спрямовано на забезпечення безперервності і послідовності оволодіння студентами навичками та вмінням професійної діяльності відповідно до вимог згідно з рівнем підготовки бакалавра. Практика проводиться відповідно до індивідуальної програми переддипломної практики, що узгоджена студентом та науковим керівником на основі загальних підходів до її змісту та структури.

Перед початком практики проводяться консультаційні збори, на яких надається вся необхідна інформація з порядку проведення переддипломної практики та консультація з техніки безпеки. За результатами зборів студенти заповнюють щоденники, в яких наводять таке: відомості про себе, назву бази практики, вид практики, період проходження практики, календарний графік із переліком запланованих до виконання робіт. Календарний графік студенти завіряють підписом керівника від університету, підписом декану факультету та печаткою факультету. За необхідності студентом на базу практики надається направлення від університету.

На першому тижні практики студент має:

отримати завдання для проходження переддипломної практики;

узгодити графік консультацій зі своїм керівником на кафедрі та ознайомитися з графіком відвідувань цієї бази практики уповноваженими викладачами-консультантами;

завірити підписом календарний графік у завідувача кафедри "Кібербезпеки та інформаційних технологій" або уповноваженою ним особою (для тих, хто проходить практику на кафедрі), або у керівника іншої бази практики (для тих, хто проходить практику за межами університету);

завірити підписом та печаткою керівництва бази практики прибуття студента на практику;

пройти інструктаж із техніки безпеки на базі практики.

На останньому тижні практики студент має:

після закінчення терміну проходження практики за результатами виконаних робіт оформити робочі записи у щоденнику та отримати відгуки керівника від кафедри та керівника від бази практики;

завірити підписом та печаткою керівництва бази практики вибуття студента з практики;

сформувати звіт, титульний аркуш якого підписати з боку студента, керівника від університету та керівника від бази практики;

якщо базою практики не є університет, то на підпис керівника від бази практики поставити печатку підприємства (організації, установи).

Індивідуальний план переддипломної практики студента має бути узгодженим із планом роботи організації, що є базою практики. У період практики студенти підкоряються всім правилам внутрішнього розпорядку і техніки безпеки, встановленим у підрозділі та на робочих місцях.

Після закінчення практики студенти оформляють всю необхідну документацію відповідно до вимог програми виробничої практики.

Загальне методичне керівництво практикою здійснюється випусковим структурним підрозділом – кафедрою "Кібербезпеки та інформаційних технологій". Загальне керівництво переддипломною практикою здійснює науковий керівник від кафедри. Для проходження практики для всіх студентів визначаються куратори від бази практики, під керівництвом яких студенти виконують поставлені в програмі завдання. Керівник переддипломної практики від кафедри надає студенту організаційне сприяння та методичну допомогу у вирішенні завдань.

Керівник практики від кафедри:

1) погоджує програму переддипломної практики і тему завдання з науковим керівником;

2) надає консультації студентам за попередньо узгодженим графіком та проводить перевірку проходження практики студентами та надає їм консультації на тих базах практики, які зазначені;

3) встановлює зв'язок із керівниками практики від організації та спільно з ними складає робочу програму проведення практики;

4) розробляє завдання згідно з темою дипломного проєкту;

5) сприяє формуванню загальної схеми виконання завдання, графіка проведення практики, режиму роботи студентів і здійснює систематичний контроль ходу практики та роботою студентів;

6) бере участь у розподілі студентів за робочими місцями або переміщення їх за видами робіт;

7) несе відповідальність разом із керівником практики від організації за дотримання студентами правил техніки безпеки;

8) здійснює контроль дотримання термінів практики та її змісту;

9) надає методичну допомогу студентам під час виконання ними індивідуальних завдань і збору матеріалів для дипломного проєкту;

10) оцінює результати виконання студентами програми практики та вносить їх як у вигляді оцінки, так і у вигляді відгуку за результатами роботи студента.

Керівник практики від бази практики:

1) погоджує програму переддипломної практики згідно зі встановленою темою дипломного проєкту;

2) надає консультації студентам щодо організації збору необхідної інформації за темою завдання;

3) встановлює зв'язок із керівниками практики від університету;

4) розробляє тематику індивідуальних завдань;

5) сприяє виконанню режиму роботи студентів і здійснює систематичний контроль проведення практики та роботи студентів;

6) бере участь у розподілі студентів за робочими місцями або переміщення їх за видами робіт;

7) несе відповідальність разом із керівником практики від університету за дотримання студентами правил техніки безпеки;

8) здійснює контроль дотримання термінів практики та її змісту;

9) оцінює результати виконання студентами програми практики та вносить їх як у вигляді оцінки, так і у вигляді відгуку за результатами роботи студента у щоденник з практики.

Науковий керівник студента:

1) координує постановку завдань із самостійної роботи студентів у період практики за виданим індивідуальним завданням зі збору необхідних матеріалів, надає відповідну консультаційну допомогу;

2) дає рекомендації щодо вивчення спеціальної літератури;

3) бере участь у роботі конференції з ведення підсумків переддипломної практики.

Студент під час проходження практики отримує від керівника практики, а також від свого наукового керівника вказівки, рекомендації та роз'яснення з усіх питань, пов'язаних з організацією та проходженням практики, звітує про виконання робіт відповідно до графіка проведення практики.

Студент:

1) проводить збір матеріалів за обраним завданням відповідно до графіка практики та режиму роботи підрозділу – місця проходження практики;

2) отримує від керівника практики вказівки, рекомендації та роз'яснення з усіх питань, пов'язаних з організацією та проходженням практики;

3) звітує про виконану роботу відповідно до встановленого графіка.

5. Оцінювання результатів практики

Оцінюють результати проходження та захисту практики за 100-бальною системою оцінювання результатів навчання, прийнятою в університеті (табл. 4).

Таблиця 4

Шкала оцінювання результатів проходження й захисту практики

Оцінка (за чотирибальною шкалою)	Оцінка (за стобальною шкалою)
Диференційована шкала	
Відмінно	90 – 100
Добре	74 – 89
Задовільно	60 – 73
Незадовільно	1 – 59
Недиференційована шкала	
Зараховано	60 – 100
Не зараховано	1 – 59

Підсумкова кількість балів, набута здобувачем вищої освіти за результатами проходження практики, враховує:

відгук керівника від бази практики;

відгук керівника від кафедри;

презентацію здобувачем вищої освіти результатів проходження практики під час захисту звіту;

відповіді на запитання.

Здобувачі вищої освіти, які не захистили у призначений термін звіти із практики, будуть мати академічну заборгованість.

Критерії оцінювання

Виробнича практика:

1 – 59 балів – виставляється в разі повної некомплектності та неякісного подання матеріалів, повної відсутності матеріалу відповідно до індивідуального завдання;

60 – 73 бали – виставляється в разі некомплектного та неякісного подання матеріалів, слабкої готовності індивідуального завдання;

74 – 89 балів – виставляється в разі наявності окремих недоробок, неповноти поданих матеріалів;

90 – 100 балів – виставляється за умови повного виконання вимог з виробничої практики у встановлений термін, готовності матеріалу згідно з індивідуальним завданням.

Переддипломна практика:

1 – 59 балів – виставляється в разі повної некомплектності та неякісного подання матеріалів, повної відсутності готовності матеріалу для включення в дипломну роботу;

60 – 73 бали – виставляється в разі некомплектного та неякісного подання матеріалів, слабкої готовності для включення в дипломну роботу;

74 – 89 балів – виставляється в разі наявності окремих недоробок, неповноти поданих матеріалів;

90 – 100 балів – виставляється за умови повного виконання вимог з переддипломної практики у встановлений термін, готовності для включення поданих матеріалів у дипломну роботу.

Рекомендована література

1. Вимоги до оформлення курсових і дипломних проєктів методичні рекомендації для студентів галузі знань 12 "Інформаційні технології" / уклад. А. А. Гаврилова, С. П. Євсеєв, Г. П. Коц, О. Г. Руденко. – Харків : ХНЕУ ім. С. Кузнеця, 2018. – 50 с.

2. ДСТУ 7093:2009. Бібліографічний запис. Скорочення слів і словосполук, поданих іноземними європейськими мовами. – Київ : Кн. палата України, 2017. – 17 с.

3. ДСТУ 3582:2013. Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила. – Київ : Мінекономрозвитку України, 2014. – 15 с.

4. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. – Київ : ДП "УкрНДНЦ", 2016. – 17 с.

5. ДСТУ 3008-15. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Київ : ДП "УкрНДНЦ", 2016. – 31 с.

6. ДСТУ 3651.0-97. Метрологія. Основні одиниці фізичних величин Міжнародної системи одиниць. Основні положення, назви та позначення. – Київ : ДП "УкрНДНЦ", 1997. – 14 с.

7. ДСТУ 1.5:2015. Національна стандартизація. Правила розроблення, викладання та оформлення нормативних документів. – Київ : ДП "УкрНДНЦ", 2015. – 65 с.

Зміст

НАВЧАЛЬНЕ ВИДАННЯ

Наскрізна програма практики
для студентів спеціальності 125 "Кібербезпека" освітньої програми "Кібербезпека" першого (бакалаврського) рівня

Самостійне електронне текстове мережеве видання

Укладачі: **Старкова** Ольга Володимирівна
Лимаренко Вячеслав Володимирович

Відповідальний за видання *О. В. Старкова*

Редактор *А. С. Ширініна*

Коректор *В. Ю. Труш*

План 2023 р. Поз. № 41 ПП. Обсяг 26 с.

Видавець і виготовлювач – ХНЕУ ім. С. Кузнеця, 61166, м. Харків, просп. Науки, 9-А

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру
ДК № 4853 від 20.02.2015 р.