МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

Кафедра кібербезпеки та інформаційних технологій

«ЗАТВЕРДЖУЮ»
Проректор
з навчально-методичної роботи
_____ №02071211

НАСКРІЗНА ПРОГРАМА ПРАКТИКИ

рівень вищої освіти другий (магістерський)
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
_____ Семенов С. Г.
(підпис) (прізвище та ініціали)

Укладачі:
_____ Старкова О. В.
(підпис) (прізвище та ініціали)
_____ Семенов С. Г.
(підпис) (прізвище та ініціали)

Харків
ХНЕУ ім. С. Кузнеця
2023

УДК 004.056(076.034)
Н31

Укладачі: О. В. Старкова
С. Г. Семенов

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» другого (магістерського) рівня [Електронний ресурс] / уклад. О. В. Старкова, С. Г. Семенов. – Харків : ХНЕУ ім. С. Кузнеця, 2023. – 15 с.

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

Рекомендовано для студентів спеціальності 125 «Кібербезпека» освітньої програми «Кібербезпека» другого (магістерського) 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», другого (магістерського) 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.

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	Заочна форма навчання	Кафедри, що забезпечують організацію	Тривалість практики	Семестри
І М	Переддипломна	+	–	Кібербезпеки та інформаційних технологій	8 тижнів	3-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	Заочна форма навчання	Кількість кредитів	Загальна кількість годин	Семестри	Форми контролю
І М	Переддипломна	+	–	12	360	3-й	звіт

1.3. Мета практик *(визначення основних завдань)*:

1.3.1. Метою переддипломної практики є узагальнення, систематизація, закріплення та поглиблення теоретичних знань студентів за профільними дисциплінами, що вивчені за спеціальністю «Кібербезпека», отримання навичок проведення аналізу сучасної системи захисту конкретного об'єкта з метою самостійного моделювання можливих кіберзагроз і 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 (НСД) 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 НСД.

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

6. Розробити вимоги щодо використання засобів захисту інформації в ІКС від витоку її технічними каналами за об'єктом управління.

1.4. Заплановані компетентності та результати навчання *(відповідно до освітньо-професійних програм)* (табл. 3):

Таблиця 3

Заплановані компетентності та результати навчання

Спеціальні компетентності	Загальні компетентності	Результати навчання
Переддипломна		
КФ10	КЗ-1, КЗ-5	РН4
КФ10	КЗ-5	РН7
КФ10	КЗ-5	РН8
КФ4, КФ10	–	РН9
КФ10	–	РН11
КФ10	–	РН12
КФ10	–	РН13
КФ10	–	РН16
КФ3, КФ4, КФ10	–	РН17
КФ4, КФ10	КЗ-1, КЗ-5	РН18
КФ1, КФ2, КФ3, КФ4, КФ6, КФ7, КФ8, КФ9	–	РН19
КФ3, КФ4, КФ7, КФ8, КФ10	–	РН21
КФ3, КФ4, КФ10	–	РН23

Примітка.

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти й удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних завдань у сфері інформаційної безпеки та/або кібербезпеки.

КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно з встановленою стратегією і політикою інформаційної безпеки та/або кібербезпеки організації.

КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів зокрема.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури в інформаційних системах, а також здатність оцінювати ефективність їхнього використання, згідно з встановленою стратегією і політикою інформаційної безпеки та/або кібербезпеки організації.

КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес-процесів / операційних процесів у галузі інформаційної безпеки та/або кібербезпеки організації загалом.

КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також ухвалювати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою вирішення складних завдань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів загалом.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес-процесів / операційних процесів, а також аналізувати і надавати оцінку ефективності їхнього використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН16. Ухвалювати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, зокрема із застосуванням сучасних методів і засобів оптимізації, прогнозування та ухвалення рішень.

РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН21. Використовувати методи натурного, фізичного та комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них у галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури й іншої доступної інформації.

2. Зміст практик

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

Студент під час проходження переддипломної практики зобов'язаний:

- повністю виконати завдання, передбачені програмою практики, з урахуванням індивідуального завдання;
- виконувати чинні на підприємстві правила внутрішнього розпорядку;
- пройти інструктаж і суворо дотримуватися правил охорони праці, техніки безпеки та виробничої санітарії;
- виконувати та нести відповідальність за виконану роботу на підприємстві за дорученням керівника практики нарівні зі штатними співробітниками;

- вести щоденник практики за етапами її проходження;
- подати на кафедру письмовий звіт про виконання переддипломної практики та індивідуального завдання разом із відгуком, підписаним керівником (куратором) практики від підприємства; захистити основні положення, відображені у звіті.

У процесі переддипломної практики студенти мають виконати такі завдання.

1. Описати напрями діяльності об'єкта управління.
2. Проаналізувати стан системи безпеки об'єкта управління.
3. Проаналізувати наявні методи реалізації несанкціонованого доступу, які можуть бути застосовані 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-комунікаційній системі від витоку її технічними каналами.

3. Вимоги до баз практик

Переддипломна практика проводиться 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 їхнього погляду придатності для проведення практики студентів за спеціальністю.

До того ж мають враховуватися перспективи сучасних напрямів розвитку ІТ-галузі, економічного, соціального та екологічного розвитку суспільства.

До підприємств – баз переддипломної практики висуваються такі вимоги:

здійснення діяльності дослідження, проєктування, впровадження й експлуатація 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 техніки та технологій, використовувати сучасну обчислювальну техніку та інформаційні технології; забезпечувати можливість проведення переддипломної практики з дотриманням програми; мати науково-технічні зв'язки з закладом вищої освіти (ЗВО).

4. Організація проведення та керівництво практикою

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.

Практика проводиться відповідно до індивідуальної програми переддипломної практики, узгодженою 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 й отримати відгуки керівника від кафедри та керівника від бази практики;

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

сформувати звіт, титульний аркуш якого підписати студенту, керівнику від університету та керівнику 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 узгоджений 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 усю необхідну документацію відповідно до вимог програми переддипломної практики.

5. Оцінювання результатів практики

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

Таблиця 4

Шкала оцінювання результатів проходження та 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, ураховує:

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 звіту із переддипломної практики:

1 – 59 балів – виставляється в разі повної некомплектності та неякісного подання матеріалів, повної відсутності готовності для включення в дипломний проєкт;

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

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 для включення поданих матеріалів у дипломний проєкт.

Рекомендована література

1. Вимоги до оформлення курсових і дипломних проектів : 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» другого (магістерського) рівня

Самостійне електронне текстове мережеве видання

Укладачі: **Старкова** Ольга Володимирівна
Семенов Сергій Геннадійович

Відповідальний за видання *О. В. Старкова*

Редактор *А. С. Ширініна*

Коректор *В. Ю. Труш*

План 2023 р. Поз. № 42 ПП. Обсяг 15 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.