МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

КІБЕРБЕЗПЕКА

Методичні вказівки
до переддипломної практики
для здобувачів другого (магістерського) рівня вищої освіти
спеціальності 125 - «Кібербезпека»

Обговорено і рекомендовано на
засіданні кафедри кібербезпеки та
математичного моделювання
Протокол №1 Від 27 серпня 2020 року

ЧЕРНІГІВ – 2020

Кібербезпека. Методичні вказівки до переддипломної практики для здобувачів другого (магістерського) рівня вищої освіти спеціальності 125 - Кібербезпека / укл: Петренко Т.А., Ткач Ю.М. – Чернігів: Національний університет «Чернігівська політехніка», 2020. – 30 с.

Укладач:

Петренко Т.А., доцент кафедри кібербезпеки та математичного моделювання, к.т.н.

Ткач Ю.М., завідувач кафедри кібербезпеки та математичного моделювання, д.пед.н., доцент

Відповідальний за випуск:

Петренко Т.А., доцент кафедри кібербезпеки та математичного моделювання, к.т.н.

Ткач Ю.М., завідувач кафедри кібербезпеки та математичного моделювання, д.пед.н., доцент

Рецензент:

Гур'єв Володимир Іванович професор кафедри кібербезпеки та математичного моделювання, к.т.н., доцент

Методичні рекомендації містять загальні положення щодо організації та проведення переддипломної практики здобувачів другого (магістерського) рівня вищої освіти спеціальності 125 - Кібербезпека. Наведено загальні положення щодо переддипломної практики, її мету, задачі та зміст, роз'яснення щодо оформлення звітної документації.

Методичні вказівки спрямовані на допомогу здобувачам вищої освіти (ЗВО) спеціальності 125- Кібербезпека та їх наукових керівників у питаннях планування, проведення та підведення підсумків практики.

ЗМІСТ

1 ВСТУП

Відповідно до освітньо-професійної програми підготовки магістрів спеціальності 125 – Кібербезпека в Національному університеті «Чернігівська політехніка» переддипломна практика є обов'язковим компонентом навчального плану.

Переддипломна практика є невід'ємною складовою і одним із завершальних етапів у підготовці висококваліфікованих фахівців у сфері кібербезпеки та захисту інформації і має на меті не тільки закріплення теоретичних знань та практичних навичок здобувачами вищої освіти, отриманих ними на етапі навчання, але і проведення досліджень в реальних умовах діяльності підприємств – баз практик, збір необхідних матеріалів для написання магістерської випускної кваліфікаційної роботи.

У період практики закладаються основи досвіду професійної діяльності, використання практичних умінь і навичок, професійних якостей особистості майбутнього фахівця з кібербезпеки за освітньо-кваліфікаційним рівнем «магістр». Практика займає важливе місце в вирішенні завдання підготовки висококваліфікованих спеціалістів, які володіють комплексом професійних знань, практичними навичками роботи за спеціальністю 125 "Кібербезпека" та необхідними організаторськими якостями.

Зміст переддипломної практики визначається діючим навчальним планом підготовки фахівців за спеціальністю 125 «Кібербезпека» та відповідними програмами з курсів «Методи побудови та аналізу криптосистем», «Методологія та організація наукових досліджень», «Стандартизація, сертифікація засобів та комплексів захисту інформації», «Проектування технічних засобів захисту інформації», «Нормативно-правове забезпечення інформаційної безпеки» та інших обов'язкових та вибіркових дисциплін. Відповідно до навчального плану підготовки магістрів спеціальності 125 – Кібербезпека в Національному університеті «Чернігівська політехніка» переддипломна практика становить з 11 кредитів (330 годин самостійної роботи студентів) та проводиться в третьому семестрів навчання. Термін проходження практики – 6 тижнів, 30 робочих днів.

Переддипломна практика проводиться згідно з Законами України „Про освіту", „Про вищу освіту", Положенням «Про проведення практики студентів вищих навчальних закладів України» затвердженим наказом Міністерства освіти України від 08.04.1993р. № 93, наказами і директивними вказівками Міністерства освіти і науки України та Положенням про проведення практики студентів Національного університету «Чернігівська політехніка» затвердженим наказом ректора ЧНТУ від 15.05.2013р. №67 та вимогами Міжнародного стандарту якості ISO серії 9000.

2 МЕТА І ЗАВДАННЯ ПРАКТИКИ

Метою практики є:

– оволодіння здобувачами вищої освіти сучасними методами, навичками, вміннями майбутньої професійної діяльності, формування у них, на базі одержаних в Національному університеті «Чернігівська політехніка» знань, професійних навичок для прийняття самостійних рішень під час роботи в конкретних суспільно-економічних умовах, виховання потреби систематично поповнювати свої знання й творчо їх застосовувати в практичній діяльності.

– закріплення, поглиблення і систематизацію теоретичних знань, отриманих під час навчання за спеціальністю 125 «Кібербезпека», в процесі реальної практичної діяльності.

– забезпечення єдності теоретичного і практичного навчання студентів з питань організації діяльності підрозділів захисту інформації, включаючи особливості функціонування підприємств та вирішуваних ними завдань, набуття студентами практичних навичок розробки пропозицій по вдосконаленню та підвищенню ефективності прийнятих технічних мір і організаційних заходів із застосуванням сучасних технологій захисту інформації, підготовка студентів до ефективного використання отриманих знань в процесі самостійного розв’язання фахових завдань. Отримання навичок проведення аналізу інформаційних систем конкретного об'єкту управління з метою самостійного проектування та розробки елементів захищених автоматизованих інформаційних систем з використанням сучасних інформаційних технологій та розвинутих інструментальних засобів захисту інформації.

Під час проходження переддипломної практики здобувачі вищої освіти розширюють на практиці набуті в ході попереднього навчання наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності 125 - Кібербезпека:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

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

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

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

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

Завдання практики:

– поглиблення, закріплення і поповнення теоретичних знань, придбаних при вивченні навчальних дисциплін за спеціальністю 125 «Кібербезпека»;

– оволодіння ЗВО сучасними методами, формами організації роботи за спеціальністю (практичними навичками з автоматизації захисту інформації, інформаційних систем та процесів, безпечного функціонування автоматизованих інформаційних систем і мереж тощо);

– отримання практичного досвіту роботи за фахом в умовах реальних підприємств та їх структурних підрозділів;

– засвоєння ЗВО на практиці структури інформаційно-аналітичної діяльності та загальнонаукових і спеціальних методів, що застосовуються в управлінні захистом інформації;

– розвиток у ЗВО професійних вмінь приймати самостійні рішення під час виконання конкретної роботи за фахом та ін.

– проведення ЗВО досліджень та збір матеріалів для подальшої підготовки та написання магістерської випускної кваліфікаційної роботи та ін.

До початку проходження практики ЗВО повинні мати базові знання з обов'язкових та вибіркових дисциплін, передбачених навчальним планом спеціальності 125 – Кібербезпека освітньо-кваліфікаційного рівня – магістр.

Переддипломна практика надає змогу здобувачам вищої освіти закріпити та поглибити навички передбачені наступними програмними результати навчання:

ПРН2. Планувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

ПРН5. Реалізовувати процеси постійної самоосвіти і професійної сертифікації, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності та ін..

3 ОРГАНІЗАЦІЯ ПЕРЕДДИПЛОМНОЇ ПРАКТИКИ

3.1 Бази практик

Переддипломна практика проводиться на підприємствах різних форм власності, в організаціях різних галузей національного господарства, в органах державної влади, наукових установах і організаціях, діяльність яких безпосередньо пов'язана з інформаційними технологіями або захистом інформації, або в структурі яких є підрозділи що забезпечують інформаційну безпеку або в штаті є посада фахівця в галузі інформаційних технологій.

Практика здобувачів вищої освіти Університету проводиться на базах, які відповідають меті, завданням, змісту практики, а також вимогам освітньо-кваліфікаційної характеристика підготовки магістрів за спеціальністю 125 - Кібербезпека.

Підприємства - бази переддипломної практики повинні мати можливість забезпечити проходження практики та виконання індивідуальних завдань ЗВО

відповідно до програми практики. На базах практики повинна функціонувати сучасне технічне обладнання, програмне забезпечення та системи зв'язку.

Список баз практики

- ТОВ «ІНТРОБОТС»;
- ТОВ «Інформаційна безпека»;
- Відділ протидії кіберзлочинам в Чернігівські області Департаменту кіберполіції НП України;
- ПАТ Чернігів обленерго;
- ТОВ "Софт Індастрі Альянс";
- Чернігівська обласна державна адміністрація та ін.

Повний список підприємств – баз практик розміщений за посиланням: https://robota-chntu.stu.cn.ua/practice/.

За згодою сторін практика може проводитися в онлайн-режимі. Організація і порядок проведення практики в онлайн-режимі передбачаються в Угоді на проведення онлайн-практики, яка укладається між Університетом і базою практики.

Практика здобувачів вищої освіти може проводитися на базі підприємств, установ та організацій, що розташовані за кордоном.

Здобувачі вищої освіти можуть запропонувати підприємство – базу проходження практики. Кафедра дає згоду про проходження практики на таких базах лише за умови, що вони відповідають вимогам для проходження переддипломної практики.

Загальна організація, керівництво та контроль за проведенням переддипломної практики здобувачів вищої освіти спеціальності 125 - Кібербезпека, освітньо-кваліфікаційного рівня магістр здійснюється відповідно до «Положення про практику», затвердженого ректором ЧДТУ 15.05.2013 року №67 відділом практики та сприяння працевлаштуванню та кафедрою кібербезпеки та математичного моделювання.

Безпосередньо організацію переддипломної практики здійснює керівник переддипломної практики (співробітник відділу практики та сприяння працевлаштуванню) та керівник практики від кафедри кібербезпеки та математичного моделювання. До керівництва практикою залучаються досвідчені викладачі кафедри.

3.2 Обов'язки керівника практики від ЧНТУ

- контроль підготовленості бази практики та вжиття, за необхідності, потрібних заходів щодо її підготовки;

- ознайомлення керівника від бази практики з програмою переддипломної практики та узгодження плану-графіку проходження практики;

- проведення організаційних зборів зі студентами, ознайомлення студентів з програмою практики, охороною праці під особистий підпис, особливостями проходження практики на підприємстві, формою звіту про результати практики;

- надання студентам-практикантам необхідних документів (направлення, програми, щоденника та ін.).

- представлення студентів та керівника практики від бази практики і участь у проведенні інструктажу з правил техніки безпеки, протипожежної безпеки та виробничої санітарії на виробництві;

- забезпечення разом з керівником від бази практики виконання програми практики;

- надання студентам допомоги в доборі матеріалу для виконання індивідуального завдання і контроль за його виконанням;

- контроль проходження практики студентами та надання необхідних консультацій з питань проходження практики;

- визначення часу і місця підведення підсумків роботи студентів та виставлення підсумкової оцінки за результатами практики;

- перевірка звітної документації і оцінка результатів виконання програми практики;

- приймання захисту практики.

3.3 Обов'язки студентів при проходженні практики

- до початку практики одержати від керівника практики кафедри інструктаж про порядок проходження практики та з техніки безпеки і консультації щодо оформлення усіх необхідних документів;

- своєчасно прибути на базу практики;

- забезпечити збір необхідного фактичного матеріалу для написання звіту про практику;

- у повному обсязі виконувати всі завдання, передбачені програмою практики і вказівками її керівників;

- вивчити і суворо дотримуватися правил охорони праці та техніки безпеки і виробничої санітарії;

- нести відповідальність за виконану роботу;

- вести записи у своїх щоденниках про характер виконуваної роботи;

- своєчасно подати необхідні звітні документи та захистити результати практики.

4 ЗМІСТ ПРАКТИКИ

Зміст переддипломної практики визначається вимогами освітньо-кваліфікаційної характеристики та освітньо-професійної програми підготовки магістрів за спеціальністю 125 - Кібербезпека.

Практиканти покроково працюють над завданнями наведеними в індивідуальній програмі практики, використовуючи знання набуті під час підготовки за спеціальністю, формують практичні навички щодо порядку проведення робіт з захисту інформації відповідно до державних стандартів на інших нормативно-правових актів України.

Для досягнення поставлених цілей та задач переддипломної практики студенти-практиканти працюють на місцях, що відповідають спеціальності 125 - Кібербезпека та рівню освітньо-професійної підготовки з урахуванням особливостей баз практики.

Оскільки під час переддипломної практики студенти отримують нові знання та практичні навички в основному при виконанні конкретних практичних завдань, то найбільш доцільною є їх робота поряд з фахівцями які працюють на штатних посадах. При цьому студенти повинні дотримуватись прийнятих на місцях проведення практики правил охорони праці і протипожежної безпеки; обов'язковим є проведенням вступного інструктажу та на кожному робочому місці.

Під час практики потрібно більш детально розглянути положення основних державних стандартів в галузі захисту інформації. Для формування вмінь та навичок у цей час особливу увагу потрібно приділити нормативним документам розроблених державною службою спеціального зв’язку та захисту інформації України. Це дасть змогу виконати завдання практики у повному обсязі.

4.1 Орієнтовний тематичний план

№	Тема програми	Год.
1.	Ознайомлення з програмою практики. Знайомство з підприємством, його структурою. Інструктаж з техніки безпеки	20
2.	Дослідження підприємства, вивчення його інформаційної діяльності, визначення об`єктів захисту – інформації з обмеженим доступом, технічного обладнання, інформаційно-комунікаційних систем і мереж, виявлення загроз, їх аналіз	20
3.	Аналіз системи забезпечення інформаційної безпеки на підприємстві. (окремо організаційний, технічний, та програмний аспекти) Виявлення слабких місць в системах захисту та уразливостей в інформаційний системі бази практики	60
4.	Розробка рекомендацій щодо вдосконалення системи захисту інформації, підвищення рівня захищеності інформації в інформаційних системах бази практики або практична реалізація і впровадження власної програмної, або інженерно-технічної розробки	100
5.	Виконання індивідуального завдання	100
6.	Підведення підсумків. Узагальнення матеріалів з практики, оформлення звіту, складання диференційного заліку	30
	Разом	330

На основі орієнтовного тематичного плану, особливостей бази практики, особистих професійних інтересів ЗВО з врахуванням запланованої теми темою майбутньої магістерської роботи керівник практики від кафедри разом зі ЗВО складає індивідуальний план проходження практики. Подальше керівництво

практикою, контроль за її виконанням здійснюється спільно керівником від бази практики та керівником від кафедри.

У кожному конкретному випадку програма переддипломної практики може змінюватись і доповнюватись для кожного здобувача вищої освіти залежно від особливостей бази практики та особистих професійних інтересів магістра.

4.2 Методичні рекомендації

1. Ознайомлення з програмою практики. Знайомство з підприємством, його структурою. Інструктаж з техніки безпеки

Практиканти повинні ознайомитися з програмою практики, її основними тематичними розділами. Отримати від керівника практики індивідуальні завдання та документи які потрібно оформити під час проходження практики.

Після прибуття на підприємство практикант повинен ознайомитися:

- з відомчим підпорядкуванням бази практики, основними нормативно-правовими документами, що лежать в основі її діяльності;
- з режимом роботи і правилами внутрішнього розпорядку;
- з вимогами, які пред'являються до працівників бази практики, їх професійних компетентностей в сфері інформаційних технологій та захисту інформації;
- з основними обов'язками працівників та посадових осіб бази практики;

Керівник установи призначає студенту керівника практики від бази практики, ознайомлює з порядком проходження, розпорядком роботи установи.

Практиканти проходять інструктаж з техніки безпеки під час проходження практики.

2. Дослідження підприємства, вивчення його інформаційної діяльності, визначення об`єктів захисту – інформації з обмеженим доступом, технічного обладнання, інформаційно-комунікаційних систем і мереж, виявлення загроз, їх аналіз

Практикантам в ході дослідження бази практики необхідно:

- провести аналіз умов функціонування підприємства, його розташування на місцевості для визначення можливих джерел загроз;
- дослідити засоби забезпечення інформаційної діяльності, які мають вихід за межі контрольованої території;
- вивчити схеми засобів і систем життєзабезпечення підприємства (електроживлення, заземлення, автоматизації, пожежної та охоронної сигналізацій), а також інженерних комунікацій та металоконструкцій;
- дослідити інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання інформації;
- визначити наявність та технічний стан засобів забезпечення технічного захисту інформації;
- перевірити наявність на підприємстві нормативних документів, які забезпечують функціонування системи захисту інформації, організацію

проектування будівельних робіт з урахуванням вимог технічного захисту інформації, а також нормативної та експлуатаційної документації, яка забезпечує інформаційної діяльності;

- виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, кіл і проводів;
- визначити технічні засоби і системи, застосування яких не обґрунтовано службовою чи виробничою необхідністю і які підлягають демонтуванню;
- визначити технічні засоби, що потребують переобладнання та встановлення засобів технічного захисту інформації.

За результатами обстеження студенти складають акт в довільній формі, який додають до звіту про проходження практики.

3. Аналіз системи забезпечення інформаційної безпеки на підприємстві (окремо організаційний, технічний, та програмний аспекти) Виявлення слабких місць в системах захисту та уразливостей в інформаційний системі бази практики

Після дослідження підприємства, вивчення його інформаційної діяльності, визначення об`єктів захисту – інформації з обмеженим доступом, технічного обладнання, інформаційно-комунікаційних систем і мереж, студенти-практиканти повинні проаналізувати програмне забезпечення ІКС що використовується для їх захисту, розглядають інженерно-технічні рішення в сфері захисту інформації. Наступним кроком практиканти повинні дослідити розпорядчі, організаційно-методичні, нормативні документи з захисту інформації що застосовуються на підприємстві, вказівки щодо їхнього застосування, інструкції, що встановлюють обов`язки, права та відповідальність персоналу.

На підставі зібраної інформації студенти-практиканти повинні зробити висновки та виявити слабкі місць в системах захисту та уразливості в інформаційний системі бази практики.

4. Розробка рекомендацій щодо вдосконалення системи захисту інформації, підвищення рівня захищеності інформації в інформаційних системах бази практики або практична реалізація і впровадження власної програмної, або інженерно-технічної розробки

На цьому етапі студентам потрібно сформувати свої пропозиції керівництву бази практики щодо вдосконалення існуючої системи захисту інформації, підвищення рівня захищеності інформації в їх інформаційних системах, тощо. А у випадку відсутності системи захисту інформації на базі практики – запропонувати кроки щодо її впровадження. При цьому потрібно зосередитися на таких напрямках забезпечення інформаційної:

- програмний захист;
- технічний захист;
- захист телекомунікаційних мереж;
- організаційний, нормативно-правовий захист, та ін.

Здобувачі вищої освіти можуть, замість підготовки рекомендацій, розробити власний програмний модуль, технічну систему, веб-додаток, тощо, використання якого підвищить рівень захищеності інформації на підприємстві – базі практики.

5. Виконання індивідуального завдання

Під час проходження практики студенти – практиканти виконують заздалегідь отримане від керівника практики індивідуальне завдання. Порядок отримання завдань та їх орієнтовна тематика наведені в п. 4.3

6. Підведення підсумків. Узагальнення матеріалів з практики, оформлення звіту, складання диференційного заліку

Практиканти закінчують виконання індивідуальних завдань практики. Оформлюють та підписують звітну документацію (щоденник практики, звіт про проходження практики, звіт про виконання індивідуального науково-дослідного завдання, додатки, відгук керівника практики від підприємства, характеристика, тощо.)

4.3 Індивідуальні завдання

Перед початком проходження переддипломної практики здобувачі вищої освіти одержують від керівника практики індивідуальні завдання, які вони повинні виконати в період проходження практики. Індивідуальні завдання розробляються відповідно до особистих професійних нахилів та уподобань ЗВО, майбутньої теми магістерської ВКР та з врахуванням прагнень ЗВО щодо майбутнього працевлаштування. Теми індивідуальних завдань видаються з урахуванням умов роботи установ – баз практики на основі теоретичних знань, які вони одержали в університеті.

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

Формами індивідуальної роботи можуть бути:

- написання рефератів на певну тему;
- підготовка тез доповідей, наукових статей;
- проведення досліджень;
- розробка програмних модулів, технічних систем або обладнання.

Індивідуальні завдання розробляються керівником практики разом з керівником магістерської ВКР. ЗВО можуть самостійно пропонувати тематику індивідуальних завдань на переддипломну практику.

Спеціальний час для написання індивідуального завдання не відводиться, воно виконується під час проходження практики.

Безпосередній керівник практики в установі бази практики надає студентам допомогу в зборі необхідного матеріалу (бланки, документи, література), контролює виконання завдання.

Орієнтовна тематика індивідуальних завдань на переддипломну практику

1. Захист користувацького контенту від копіювання на Web-ресурсі.
2. Забезпечення цілісності та доступності Web-серверів.
3. Захист інформації в системах електронного документообігу.
4. Технічні системи контролю та управління доступом до приміщень.
5. Захист інформації засобами операційних систем.
6. Тестів на проникнення.
7. Моніторинг ризиків кібербезпеки.
8. Захист інформації при використанні електронної пошти.
9. Захист інформації у телекомунікаційних системах.
10. Системи захисту баз даних.
11. Захист Internet of Things.
12. Автентифікація, ідентифікація та авторизація в системах захисту інформації.
13. Протидії інформаційно-психологічним впливам.
14. Аналіз систем менеджменту інформаційної безпеки підприємства.
15. Ризики інформаційної безпеки підприємства.
16. Система управління персоналом з питань інформаційної безпеки підприємства.
17. Захист бездротових мереж.
18. Технічні системи захисту інформації.
19. Управління мережевою безпекою.
20. Безпека в хмарних технологіях.
21. Етичний хакінг та ін.

5 ФОРМИ І МЕТОДИ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ СТУДЕНТІВ

Поточний контроль здійснюється керівником практики від бази практики, з залученням у разі необхідності керівника практики від кафедри шляхом оцінювання якості роботи здобувачів вищої освіти на базі практики під час виконання навчальних та індивідуального завдання. При цьому оцінюється рівень теоретичної та практичної підготовки практикантів до вирішення конкретних завдань, їх дисциплінованість, пунктуальність, ініціативність, самостійність а також повнота, своєчасність та правильність виконання завдань, рівень

Підсумковий контроль проводиться керівником практики від кафедри у вигляді захисту практики студентом. В ході захисту результатів практики ЗВО надають оформлені відповідно до вимог документи про проходження практики (щоденник, звіт, індивідуальне завдання), звітують про результати своєї роботи

під час проходження переддипломної практики, представляють результати виконання індивідуального завдання.

6 ПІДБИТТЯ ПІДСУМКІВ ПРАКТИКИ

Після закінчення строку проходження практики студенти у письмовому вигляді звітують про виконання індивідуального плану проходження практики та індивідуального завдання практики. Загальна і характерна форма звітності студента за практику – це подання письмового звіту, підписаного і оціненого безпосередньо керівником від бази практики, а також керівником практики від кафедри. Письмовий звіт разом з іншими документами (звітом, щоденником, характеристикою, рецензіями тощо) подається на рецензування керівникові практики від кафедри.

Додатки 1-6 містять зразки договору, повідомлення, листа-направлення на практику та зразки звітних документів: щоденник, титульну сторінку звіту, відгук і зауваження керівника практики.

У звіті мають бути відомості про виконання студентом усіх розділів програми практики та індивідуального завдання, розділи з охорони праці та техніки безпеки, висновки та пропозиції, список використаних джерел. Оформлюється звіт відповідно до загальних вимог [3, 4].

Здобувачі вищої освіти звітують про проходження практики перед комісією, призначеною завідуючим кафедрою, до складу якої входять керівники практики від кафедри. Комісія приймає звіт у здобувачів вищої освіти на базах практики в останні дні її проходження або в університеті протягом перших трьох днів після закінчення практики. Оцінка за практику вноситься до заліково-екзаменаційної відомості і індивідуального навчального плану здобувача вищої освіти за підписами членів комісії. Залікові відомості з практик, що проводяться влітку, викладач підписує та здає особисто в дирекцію протягом перших трьох днів після закінчення практики.

Оцінювання результатів практики здійснюється за національною шкалою та шкалою ECTS. При цьому оцінюється дисциплінованість студентів-практикантів під час відвідування бази практики, вчасність, повнота, якість і самостійність виконання індивідуальних завдань а також загальний рівень теоретичної та практичної підготовки студентів-практикантів.

Шкала відповідності оцінок ECTS

Відсотки підсумкової оцінки	Оцінка за національною шкалою	Оцінка за шкалою ECTS	Обґрунтування оцінки
1	2	3	4
90-100	Відмінно	A	Відмінне виконання завдань лише з незначною кількістю помилок
82–89	Добре	B	Контрольні заходи виконані вище середнього рівня з кількома помилками.

1	2	3	4
75–81	Добре	C	В цілому правильна робота з певною кількістю незначних помилок
67–74	Задовільно	D	Контрольні заходи виконані непогано, але зі значною кількістю недоліків.
60–66		E	Виконання контрольних заходів задовольняє мінімальним критеріям.
1–59	Незадовільно	FX	Студенту надається можливість скласти оговорені контрольні заходи для поліпшення підсумкової оцінки

Результати оцінювання практики можуть бути оскаржені здобувачами вищої освіти у порядку, що регламентується «Положенням про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка».

Здобувачу вищої освіти, який не приступив до практики своєчасно з поважних причин призначається проходження практики в інший період (відповідно до індивідуального графіку та наказу ректора).

У разі отримання незадовільної оцінки за проходження практики, ліквідація заборгованості здійснюється у порядку, що регламентується «Положенням про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка»».

Підсумки проведення переддипломної практики, після її закінчення обговорюються на засіданні кафедри кібербезпеки та математичного моделювання.

7 РЕКОМЕНДОВАНІ ІНФОРМАЦІЙНІ ДЖЕРЕЛА

1. Андреев В.І. Стратегія управління інформаційною безпекою: підручник / В.І.Андреев, В.Д.Козюра, Л.М.Скачек, В.О.Хорошко. – К.: Вид. ДУІКТ, 2007. – 277 с.
2. Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов / Е.Б.Белов, В.П.Лось, Р.В.Мещеряков. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 544 с.
3. Блавацька Н.М. Програмне забезпечення систем захисту інформації: підручник / Н.М.Блавацька, В.Д.Козюра, В.О.Хорошко. – К.: Вид. ДУІКТ, 2011. – 330 с.
4. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебное пособие для студентов высших учебных заведений / Г.А.Бузов, С.В.Калинин, А.В.Кондратьев. – М.: «Горячая линия – Телеком», 2005. – 416 с.
5. Гайворонський М.В. Безпека інформаційно-комунікаційних систем. - К.: Видавнича група BHV, 2009. - 608 с.

6. Грибунин В.Г. Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений / В.Г.Грибунин, В.В.Чудовский. – М.: Издательский центр «Академия», 2009. – 416 с.
7. Довгань О.Д. Методологія захисту інформації: навч.-метод. посіб. / О.Д.Довгань, Г.М.Гулак, А.К.Гринь, С.В.Мельник. – К.: Наук.-вид. центр НА СБ України, 2012. – 184 с.
8. Железняк В.К. Защита информации от утечки по техническим каналам: учебное пособие / В.К.Железняк. – СПб.: ГУАП., 2006. – 188 с.
9. Зайцев А.П. Технические средства и методы защиты информации: Учебник для вузов / А.П.Зайцева, А.А.Шелупанов, Р.В.Мещеряков и др.; – М.: ООО «Издательство Машиностроение», 2009. – 508 с.
10. Коженевский С.Р. Термінологічний довідник з питань технічного захисту інформації / С.Р.Коженевский, Г.В.Кузнецов, В.О.Хорошко, Д.В.Чирков; за ред. проф. В.О.Хорошка. – К.: Вид. ДУІКТ, 2007. – 365 с.
11. Конахович Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф.Конахович, В.П.Климчук, С.М.Паук, В.Г.Потапов. – К.: «МК-Пресс», 2005. – 288 с.
12. Конеев И.Р. Информационная безопасность предприятия / И.Р.Конеев, А.В.Беляев. – СПб.: БХВ-Петербург, 2003. – 752 с.
13. Куприянов А.И. Основы защиты информации: учеб. пособие для студ. высш.учеб. заведений / А.И.Куприянов, А.В.Сахаров, В.А.Шевцов. – М.: Изд. центр «Академия», 2006. – 256 с.
14. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для студ. высш. учеб. заведений / В.П.Мельников, С.А.Клейменов – 3-е изд., стер. – М.: Изд. центр «Академия», 2008. – 336 с.
15. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / В.Ф.Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.
16. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов, 2 -е изд. / В.И.Ярочкин. – М.: Академический Проект; Гаудеамус, 2004. – 544 с.

8 НОРМАТИВНІ ДОКУМЕНТИ

1. Про вищу освіту [Текст]: Закон України № 1556-VII від 01.07.2014 // Відомості Верховної Ради, 2014, № 37-38, ст. 2004.

2. Положення про проведення практики здобувачів вищої освіти Національного університету «Чернігівська політехніка» затв. Вченою радою НУ «Чернігівська політехніка» 31 серпня 2020 р. протокол № 6 Введено в дію наказом ректора від 31 серпня 2020 р. № 26. - Чернігів - 2020

3. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання: ДСТУ ГОСТ 7.1:2006. Чинний від 07.01.2007. - К. : Держспоживстандарт України, 2007. - 47 с.

4. Оформлення наукових джерел відповідно до вимог Вищої атестаційної комісії України [Електронний ресурс] // Вища атестаційна комісія України. – 2019. – Режим доступу до ресурсу: https://vak.in.ua.

5. Правила забезпечення захисту інформації в інформаційних телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою КМУ від 29 березня 2006. - №373.

6. Державний стандарт України Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96

7. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

8. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

9. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.

10. НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.

11. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

12. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення.

13. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.

14. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

15. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

16. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

17. НД ТЗІ 2.7-011-12 Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв.

18. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи.

19. НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

20. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

21. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

9 ДОДАТКИ

Додаток 1.
Договір
на проведення практики студентів
Національного університету «Чернігівська політехніка»
№ __ ___

м. Чернігів *“___” _____ 202__ р.*

Національний університет «Чернігівська політехніка» (надалі - навчальний заклад), в особі ректора _____, який діє на підставі статуту, з однієї сторони і _____ _____ (надалі – база практики) в особі _____, який діє на підставі _____ з другої сторони, уклали цей договір на проведення практики студентів Національного університету «Чернігівська політехніка» (надалі - Договір), разом іменовані – Сторони, а кожна окремо – Сторона, про наступне:

І. ПРЕДМЕТ ДОГОВОРУ

1. Забезпечення на умовах взаємовигідного співробітництва Сторін організації проходження практики студентами університету відповідно до умов цього Договору.

ІІ. ОБОВ’ЯЗКИ І ВІДПОВІДАЛЬНІСТЬ СТОРІН

2. База практики зобов’язується:

2.1. Належним чином виконувати умови цього Договору.

2.2. Відмовляти в організації проходження практики тим студентам, відповідно до яких не виконуються умови п. 3 р.2 Договору.

2.3. Коригувати чисельність студентів в залежності від можливостей.

2.4. Прийняти студентів на практику згідно з календарним планом.

2.5. Надіслати до вищого навчального закладу повідомлення встановленого зразка про прибуття на практику студента(ів).

2.6. Призначити наказом кваліфікованих спеціалістів для безпосереднього керівництва практикою.

2.7. Створити необхідні умови для виконання студентами програм практики, не допускати їх використання на посадах та роботах, що не відповідають програмі практики та майбутній спеціальності.

2.8. Забезпечити студентам умови безпечної роботи на кожному робочому місці. Проводити обов’язкові інструктажі з охорони праці, ввідний та на робочому місці. У разі потреби навчати студентів-практикантів безпечним методам праці.

2.9. Надати студентам-практикантам і керівникам практики від навчального закладу можливість користуватись документацією, необхідною для виконання програми практики.

2.10. Забезпечити облік виходів на практику студентів-практикантів. Про всі порушення трудової дисципліни, внутрішнього розпорядку та про інші порушення повідомляти навчальний заклад.

2.11. Після закінчення практики дати характеристику на кожного студента-практиканта, у якій відобразити якість підготовленого ним звіту.

3. Вищий навчальний заклад зобов'язується:

3.1. Ознайомити базу практики з програмою практики через студента-практиканта, не пізніше ніж за тиждень – надати базі практики список студентів, які направляються на практику.

3.2. Призначити керівниками практики кваліфікованих викладачів.

3.3. Забезпечити додержання студентами трудової дисципліни і правил внутрішнього трудового розпорядку. Брати участь у розслідуванні комісією бази практики нещасних випадків, якщо вони сталися з студентами під час проходження практики.

4. Відповідальність сторін за невиконання угоди

4.1. Сторони відповідають за невиконання покладених на них обов'язків щодо організації і проведення практики згідно з законодавством про працю в Україні.

4.2. Всі суперечки, що виникають між сторонами за цим Договором вирішуються в установленому порядку.

5. Прикінцеві положення:

5.1. Договір набирає чинності з дня його підписання Сторонами і діє до _____.

5.2. У разі відсутності заяви однієї зі Сторін про припинення або зміну цього Договору після закінчення строку його чинності протягом одного місяця, Договір вважається продовженим на той самий строк і на тих самих умовах.

5.3. Зміни та доповнення до цього Договору можуть бути внесені за взаємною згодою Сторін, що оформляється додатковим договором до цього Договору.

5.4. Договір складений у двох примірниках – по одному для кожної Сторони.

6. Юридичні адреси сторін:

Навчального закладу: 14027, м. Чернігів, вул. Шевченка, 95, Тел.: (04622)31651, Факс: (04622) 3 42 44, E-mail: cstu@stu.cn.ua;

Бази практики:

_____

_____

_____

Підписи та печатки:

Ректор Національного університету «Чернігівська політехніка»	_____ (посада) _____
_____ /_____/ (підпис) (прізвище, ініціали)	_____ /_____/ (підпис) (прізвище, ініціали)
«____» _____ 20__ р.	«____» _____ 20__ р.
М.П.	М.П.

Додаток 2. Направлення на практику

КЕРІВНИКУ

_____
_____
_____
_____
_____

НАПРАВЛЕННЯ НА ПРАКТИКУ

/є підставою для зарахування на практику/

Згідно з угодою від „___” _____ 20__ року № ___, яку укладено з

_____
_____

(повне найменування підприємства, організації, установи)

направляємо на практику студентів ____ курсу, які навчаються за напрямом підготовки (спеціальністю) _____
_____

Назва практики

_____

Строки практики з „___” _____ 20___ року
по „___” _____ 20 ___ року

Керівник практики від кафедри_____
_____

(посада, прізвище, ім’я, по батькові)

ПРІЗВИЩА, ІМЕНА ТА ПО БАТЬКОВІ СТУДЕНТІВ

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

М.П.

Керівник переддипломної практики
Національного університету
«Чернігівська політехніка» _____ _____

(підпис) (прізвище та ініціали)

Додаток 3. Повідомлення про прибуття на практику

ПОВІДОМЛЕННЯ

студент Національного університету «Чернігівська політехніка»

_____

(прізвище, ім'я, по батькові)

_____

(курс, інститут, факультет (відділення), напрям підготовки (спеціальність))

прибув „___" _____ 20___ року до _____

(назва підприємства, організації, установи)

_____

і приступив до практики. Наказом по підприємству (організації, установі) від „__" _____20____ року № _____ студент ___

прийнятий на практику_____

(назва структурного підрозділу)

_____

Керівником практики від підприємства (організації, установи) призначено

_____

(посада, прізвище, ім'я, по батькові)

Керівник підприємства (організації, установи)

_____ _____

(підпис) (посада, прізвище, ім'я, по батькові)

Печатка (підприємства, організації, установи)

"_____"_____ 20___ року

Керівник практики від кафедри Національного університету «Чернігівська політехніка» _____

_____

(назва кафедри)

_____ _____

(підпис) (посада, прізвище, ім'я, по батькові)

"_____"_____20____ року

Додаток 4. Щоденник практики

Національний університет «Чернігівська політехніка»

ЩОДЕННИК ПРАКТИКИ

_____

(вид і назва практики)

студента _____

(прізвище, ім’я, по батькові)

ННІ _____

Кафедра _____

освітньо-кваліфікаційний рівень_____

спеціальність_____

(назва)

_____ курс, група _____

Студент_____
(прізвище, ім’я, по батькові)

прибув на підприємство, організацію, установу _____
_____

Печатка
підприємства, організації, установи ,,____” _____ 20___ року

_____ _____
(підпис) (посада, прізвище та ініціали відповідальної особи)

Вибув з підприємства, організації, установи _____
_____

Печатка
Підприємства, організації, установи “____” _____ 20___ року

_____ _____
(підпис) (посада, прізвище та ініціали відповідальної особи)

Календарний графік проходження практики

№ з/п	Назви робіт	Тижні проходження практики						Відмітки про виконання
		1	2	3	4	5	6	
1	2	3	4	5	6	7	8	9

Керівники практики
від кафедри Національного університету
«Чернігівська політехніка» _____ _____
(підпис) (прізвище та ініціали)

від підприємства, організації, установи _____ _____
(підпис) (прізвище та ініціали)

Робочі записи під час практики

Відгук і оцінка роботи студента на практиці

_____

(назва підприємства, організації, установи)

Керівник практики від підприємства, організації, установи _____

_____

_____ _____

(підпис) (прізвище та ініціали)

Печатка

«_____» _____ 20 __ року

Відгук осіб, які перевіряли проходження практики

Висновок керівника практики від кафедри Національного університету «Чернігівська політехніка» про проходження переддипломної практики

Дата складання заліку „____”_____20____ року

Оцінка:
за національною шкалою_____
(словами)

кількість балів _____
(цифрами і словами)

за шкалою ECTS _____

Керівник практики від кафедри Національного університету
«Чернігівська політехніка» _____ _____
(підпис) (прізвище та ініціали)

Додаток 5. Титульна сторінка звіту про виконання програми переддипломної практики

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

ЗВІТ

про виконання програми переддипломної практики

студента _____
(прізвище, ім'я, по батькові)

групи _____

спеціальність _____

спеціалізація _____

кваліфікаційний рівень _____

база практики _____
(повна назва)

Керівник практики
від бази практики

_____
(посада, прізвище, ініціали)

Керівник практики від кафедри

_____
(посада, прізвище, ініціали)

Чернігів – НУ «Чернігівська політехніка» - 20__

Додаток 6.

Відгук і зауваження керівника практики

_____

(текст відгуку)

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Керівник практики від підприємства,
установи організації: _____

_____

(посада)

_____ _____

(підпис) (П.І.П.)

Для нотатків