

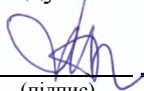


Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут
електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

РОБОЧА ПРОГРАМА
Переддипломна практика

ЗАТВЕРДЖУЮ

Завідувачка кафедри


_____ Ткач Ю.М.
(підпис) (прізвище та ініціали)
27 серпня 2025р..

Розробник: Петренко Тарас Анатолійович, доцент кафедри кібербезпеки та математичного моделювання, к.т.н. _____


Силабус обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від 26 серпня 2025р. №6

Узгоджено з гарантом освітньої програми: _____
 _____ Ткач Ю.М.

1. Загальна інформація про дисципліну

Тип дисципліни	Обов'язкова
Мова викладання	Українська
Рік навчання та семестр	Денна та заочна форма навчання: другий рік, перший семестр. 125/F5 Кібербезпека та захист інформації ОПП Кібербезпека
Викладач (-і)	Петренко Тарас Анатолійович, доцент кафедри кібербезпеки та математичного моделювання, кандидат технічних наук
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/ https://scholar.google.com.ua/citations?user=2bJE-4IAAAAJ&hl https://www.linkedin.com/in/taraspetsenko/ https://orcid.org/0000-0001-5571-3815 https://www.webofscience.com/wos/author/record/ABA-8146-2021 https://www.scopus.com/authid/detail.uri?authorId=57193026484
Контакти викладача	+380504650364, mail_taras@stu.cn.ua
Сторінка курсу в системі дистанційного навчання	https://eln.stu.cn.ua/course/view.php?id=4413

2. Анотація курсу.

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 кваліфікаційної роботи. Переддипломна практика – одна з найбільш важливих освітніх компонент підготовки кваліфікованого фахівця з кібербезпеки яка є зв'язуючою ланкою окремих дисциплін з кваліфікаційною роботою магістра та подальшим працевлаштуванням за фахом.

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 F5 Кібербезпека та захист інформації та необхідними організаторськими якостями.

3. Мета та цілі курсу.

Мета переддипломної практики:

- 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/F5 Кібербезпека та захист інформації, в процесі реальної практичної діяльності.

- забезпечення єдності теоретичного і практичного навчання здобувачів вищої освіти з питань організації діяльності підрозділів захисту інформації, включаючи особливості функціонування підприємств та вирішуваних ними завдань, набуття здобувачами вищої освіти практичних навичок розробки пропозицій по вдосконаленню та підвищенню ефективності прийнятих технічних мір і організаційних заходів із застосуванням сучасних технологій захисту інформації, підготовка здобувачів вищої освіти 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.

Завдання практики:

- поглиблення, закріплення і поповнення теоретичних знань, придбаних при вивченні навчальних дисциплін за спеціальністю F5 Кібербезпека та захист інформації;

- оволодіння здобувачами вищої освіти 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 досвіду роботи за фахом в умовах реальних підприємств та їх структурних підрозділів;

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

- розвиток у здобувачами вищої освіти професійних вмінь приймати самостійні рішення під час виконання конкретної роботи за фахом та ін.

– проведення здобувачами вищої освіти досліджень та збір матеріалів для подальшої підготовки та написання магістерської кваліфікаційної роботи та ін.

4. Результати навчання

Під час проходження переддипломної практики здобувачі вищої освіти розширюють на практиці набуті в ході попереднього навчання наступні загальні та фахові компетентності, передбачені освітньою програмою спеціальності F5 Кібербезпека та захист інформації:

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Здатність проводити дослідження на відповідному рівні.

КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

КЗ6. Здатність до ініціативності, відповідальності та навички до превентивного і аварійного планування, управління заходами безпеки професійної діяльності, уміння приймати рішення у складних та непередбачуваних ситуаціях, лідерські якості та знання міжнародних норм і законодавства України у сфері безпеки життєдіяльності населення, системи управління охороною праці та цивільного захисту

КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

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

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

ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

ПРН17. 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.

ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.

ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

ПРН24. Забезпечувати гарантії збереження здоров'я і працездатності працівників у виробничих умовах через ефективне управління охороною праці та формування

відповідальності за колективну та власну безпеку; використовувати методи превентивного та аварійного планування, керувати заходами з безпеки професійної діяльності, приймати рішення у складних та непередбачуваних ситуаціях, вирішувати професійні завдання з урахуванням вимог цивільного захисту та охорони праці

5. Пререквізити

Передумовою для проходження переддипломної практики є успішне засвоєння дисциплін передбачених освітньою-професійною програмою Кібербезпека другого (магістерського) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації. Дисципліна є базовою для підготовки кваліфікаційної роботи магістра та подальшої успішної професійної діяльності за спеціальністю.

6. Обсяг курсу.

Вид заняття	Загальна кількість годин (очно/заочна форма навчання)
Лекції	-/-
Лабораторні заняття	-/-
Самостійна робота	480/480
Індивідуальне завдання – дослідження та систематизація інформаційних джерел для написання кваліфікаційної роботи	
Всього кредитів	16/16

Консультації керівників практики та захист практики – дистанційно в MS Teams та очно в лабораторії кафедри.

Самостійна робота – дистанційно або очно на підприємстві-базі практики з використанням системи дистанційного навчання університету, рекомендованих інформаційних джерел, презентацій, нормативно-правових актів тощо.

7. Перелік баз практики

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/F5 Кібербезпека та захист інформації.

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.

Орієнтовний список баз практики

- ТОВ «Інформаційна безпека»;
- Департамент кіберполіції Національної поліції України
- ПАТ Чернігівобленерго;
- ТОВ “Софт Індастрі Альянс”;
- Чернігівська обласна державна адміністрація;
- Кафедра кібербезпеки та математичного моделювання НУ «Чернігівська політехніка» та ін.

Повний список підприємств – баз практик розміщений за посиланням:
<https://surl.li/adulbn>

З базами практики (підприємствами, організаціями, установами будь-яких форм власності) НУ «Чернігівська політехніка» завчасно укладає угоди на її проведення за встановленою формою, тривалість дії таких договорів може бути до п'яти років.

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/F5 Кібербезпека та захист інформації, освітньо-кваліфікаційного рівня магістр здійснюється відповідно до [«Положення про проведення практики здобувачів вищої освіти Національного університету «Чернігівська політехніка»](#) Затвердженого Вченою радою НУ «Чернігівська політехніка» 31 серпня 2020р., протокол № 6 та введено в дію наказом ректора № 26 від 31 серпня 2020р. центром розвитку кар'єри 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.

8. Тематика курсу

Зміст переддипломної практики визначається вимогами освітньо-кваліфікаційної характеристики та освітньо-професійної програми підготовки магістрів за спеціальністю F5 Кібербезпека та захист інформації.

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 F5 Кібербезпека та захист інформації а рівню освітньо-професійної підготовки з урахуванням особливостей баз практики.

Оскільки під час переддипломної практики здобувачі вищої освіти 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 здобувачі вищої освіти 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.

Орієнтовний тематичний план

№	Тема програми	Год.
1.	Ознайомлення з програмою практики. Знайомство з підприємством, його структурою. Інструктаж з техніки безпеки	30
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	50

№	Тема програми	Год.
3.	Аналіз системи забезпечення інформаційної безпеки на підприємстві. (окремо організаційний, технічний, та програмний аспекти) Виявлення слабких місць в системах захисту та уразливостей в інформаційній системі бази практики	50
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	200
6.	Підведення підсумків. Узагальнення матеріалів з практики, оформлення звіту, складання диференційного заліку	50
	Разом	480

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 календарний 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.

9. Система оцінювання та вимоги

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

Після закінчення строку проходження практики здобувачі вищої освіти у письмовому вигляді звітують про виконання індивідуального плану проходження практики та індивідуального завдання практики. Загальна і характерна форма звітності здобувачів вищої освіти 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. У звіті мають бути відомості про виконання здобувачем вищої освіти 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.

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 в АС Деканат керівником практики від кафедри. 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.

Результат роботи здобувача вищої освіти	Особливості оцінювання	Бали
---	------------------------	------

Звітна документація, самостійність, пунктуальність, оформлення	При перевірці та оцінюванні звіту про проходження переддипломної практики враховується повнота правильності виконання завдань передбачених програмою практики, самостійність виконання, терміни здачі та відповідність оформлення звітної документації діючим вимогам. Максимальна кількість балів 30.	30
Індивідуальне завдання	Індивідуальне завдання оцінюється від 0 до 30 балів. Кількість балів залежить від рівня теоретичних знань та практичних навичок здобувача вищої освіти, самостійності виконання та повноти опрацювання теми індивідуального завдання	30
Підсумковий контроль	Захист практики. Оцінюються відповіді здобувачів вищої освіти на питання керівника практика	40

Діяльність ЗВО та форма контролю	Кількість балів	
Якість виконання програми практики та звітної документації	0	10
Самостійність виконання програми практики	0	10
Своєчасність виконання завдань передбачених програмою практики	0	5
Відповідність оформлення звітної документації встановленим критеріям	0	5
Індивідуальне завдання	0	30
Залік (захист практики)	0	40

Шкала оцінювання результатів навчання

Оцінка в балах	Оцінка ECTS	Оцінка за національною шкалою (диференційований залік)	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	A (відмінно)	відмінно	зараховано
82-89	B (дуже добре)	добре	
75-81	C (добре)		
66-74	D (задовільно)	задовільно	
60-65	E (достатньо)		
0-59	FX (незадовільно)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

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 захист практики, ліквідація заборгованості здійснюється у порядку, що регламентується Положенням про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка»

<https://stu.cn.ua/wp-content/stumedia/normobaza/normdoc/norm-osvitproces/polozhennya-pro-potoch>

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

10. Обладнання та програмне забезпечення

Для проходження практики використовується наявне на базі практики обладнання для захисту інформації, комп'ютери, апаратне та програмне забезпечення, інформаційно-комунікаційні системи. Для оформлення звіту з практики використовується програмне забезпечення Microsoft Office, Open Office або аналогічне.

11. Політики курсу

Вивчення курсу базується на принципах взаємної поваги й довіри викладача та здобувача вищої освіти, рівноправності й толерантності.

Академічна доброчесність - самостійність виконання навчальних завдань та посилання на джерела у випадку використання напрацювань інших авторів. Види порушень академічної доброчесності - академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво.

Відповідно до [Кодексу академічної доброчесності Національного університету «Чернігівська політехніка»](#) за порушення академічної доброчесності здобувачі освіти можуть мати наслідком: повторне проходження підсумкового оцінювання; повторне вивчення відповідного освітнього компонента освітньої програми; - відрахування з Університету; позбавлення академічної стипендії.

Політика дедлайнів - своєчасність здачі практичного завдання оцінюється в 1 бал за кожне завдання. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоечасної здачі зазначених робіт (хвороба, відсутність електроенергії чи зв'язку, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом).

Політика перезарахування кредитів у випадку мобільності - перезарахування кредитів проводиться відповідно до [Порядку визначення академічної різниці та визнання результатів попереднього навчання в Національному університеті «Чернігівська політехніка»](#) та [Положення про академічну мобільність учасників освітнього процесу Національного університету «Чернігівська політехніка»](#)

Політика щодо відвідування - відвідування занять є обов'язковим. При наявності поважних причин (хвороба, участь в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом) студенти можуть узгодити з викладачем індивідуальний графік навчання та здачі всіх видів навчальної роботи. Студенти можуть перескладати або відпрацьовувати пропущені заняття на консультаціях викладача чи у спеціально відведений викладачем для цього час.

Здобувач вищої освіти, який має більше 30% пропусків навчальних занять (без поважних причин) від загального обсягу аудиторних годин згідно з індивідуальним начальним планом не допускається до складання екзамену під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому [Положенням про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка»](#)

Політика щодо правил поведінки на заняттях - активна участь у навчальному процесі, виконання необхідного мінімуму навчальної роботи, коректна поведінка щодо інших учасників навчального процесу, взаємоповага, використання мобільних пристроїв та комп'ютерної техніки тільки для навчання.

Політика заохочень та стягнень. Результати навчальної, наукової та організаційної діяльності студентів за напрямками курсу їм можуть нараховуватися додаткові бали - до 10 балів, в залежності від вагомості досягнень студента. Види позанавчальної діяльності, за які студенти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, статті на науково-практичних конференціях, винаходи, патенти, авторські

свідомості за напрямками курсу.

Політика оскарження результатів контрольних заходів. Для вирішення спірних питань, пов'язаних із організацією та проведенням семестрового контролю, оцінювання практик, атестації та визнанні результатів навчання в неформальній та/або інформальній освіті на факультеті створюється апеляційна комісія розпорядженням декана, до складу якої включаються, завідувачі кафедр, науково-педагогічні працівники та представники органів студентського самоврядування. Головою апеляційної комісії призначається декан. Порядок подання та розгляду апеляцій визначається відповідно до п.7 [Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка»](#).

12. Рекомендована література та інформаційні джерела

1. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006.

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

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

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

4. 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.

5. Система дистанційного навчання НУ «Чернігівська політехніка». – [Електронний ресурс]. – Режим доступу: <https://eln.stu.cn.ua/course/view.php?id=4413>

6. Центр розвитку кар'єри.– [Електронний ресурс]. – Режим доступу: <http://robota-chntu.stu.cn.ua/>

7. Державна служба спеціального зв'язку та захисту інформації України. – [Електронний ресурс]. – Режим доступу: <https://cip.gov.ua/ua>