

Міністерство освіти і науки України  
Національний технічний університет  
«Дніпровська політехніка»

Кафедра безпеки інформації та телекомунікацій

**«ЗАТВЕРДЖЕНО»**  
на засіданні кафедри БІТ  
(протокол № 9 від 23.04.2019р.)  
завідувач кафедри  
Корнієнко В.І. \_\_\_\_\_

**РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**  
**«Основи забезпечення безпеки інформації»**

Галузь знань .....	12 Інформаційні технології
Спеціальність .....	125 Кібербезпека
Освітній рівень.....	бакалавр
Освітньо-професійна програма	Кібербезпека
Спеціалізація .....	
Статус .....	
Загальний обсяг .....	5 кредитів ЄКТС (150 годин)
Форма підсумкового контролю	диференційний залік
Термін викладання .....	3-й семестр
Мова викладання .....	українська

Викладач: ас. Мілінчук Ю.А.

Пролонговано: на 20\_\_/20\_\_ н.р. \_\_\_\_\_ (\_\_\_\_\_) «\_\_» 20\_\_р.  
(підпис, ПІБ, дата)

на 20\_\_/20\_\_ н.р. \_\_\_\_\_ (\_\_\_\_\_) «\_\_» 20\_\_р.  
(підпис, ПІБ, дата)

Дніпро  
НТУ «ДП»  
2019

Робоча програма навчальної дисципліни «Основи забезпечення безпеки інформації» для бакалаврів за освітньо-професійною програмою «Кібербезпека» / Нац. техн. ун-т. «Дніпровська політехніка», каф. безп. інф. та телеком. – Д.: НТУ «ДП», 2019. – 8 с.

Розробник – Мілінчук Ю.А.

Робоча програма регламентує:

- мету дисципліни;
- дисциплінарні результати навчання, сформовані на основі трансформації очікуваних результатів навчання освітньої програми;
- базові дисципліни;
- обсяг і розподіл за формами організації освітнього процесу та видами навчальних занять;
- програму дисципліни (тематичний план за видами навчальних занять);
- алгоритм оцінювання рівня досягнення дисциплінарних результатів навчання (шкали, засоби, процедури та критерії оцінювання);
- інструменти, обладнання та програмне забезпечення;
- рекомендовані джерела інформації.

Робоча програма призначена для реалізації компетентнісного підходу під час планування освітнього процесу, викладання дисципліни, підготовки студентів до контрольних заходів, контролю провадження освітньої діяльності, внутрішнього та зовнішнього контролю забезпечення якості вищої освіти, акредитації освітніх програм у межах спеціальності.

Погоджено рішенням методичної комісії спеціальності 125 Кібербезпека (протокол № 8 від 23.04.2019).

## ЗМІСТ

1 МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ .....	4
2 ОЧІКУВАНІ ДИСЦИПЛІНАРНІ РЕЗУЛЬТАТИ НАВЧАННЯ .....	4
3 БАЗОВІ ДИСЦИПЛІНИ .....	4
4 ОБСЯГ І РОЗПОДІЛ ЗА ФОРМАМИ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ ТА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ .....	5
5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ .....	5
6 ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ .....	6
6.1 Шкали .....	6
6.2 Засоби та процедури .....	6
6.3 Критерії .....	7
7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ .....	8
8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ .....	8

## 1 МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

В освітньо-професійній програмі Національного технічного університету «Дніпровська політехніка» спеціальності 125 «Кібербезпека» здійснено розподіл програмних результатів навчання (ПРН) за організаційними формами освітнього процесу. Зокрема, до дисципліни Ф14 «Кібербезпека» віднесено такі результати навчання:

CP1	<ul style="list-style-type: none"><li>- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки;</li><li>- розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем;</li><li>- виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.</li></ul>
CP5	<ul style="list-style-type: none"><li>- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації;</li><li>- проектувати та реалізовувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації;</li><li>- визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;</li></ul>
CP9	<ul style="list-style-type: none"><li>- забезпечувати функціонування системи управління інформаційною та\або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки;</li></ul>
CP11	<ul style="list-style-type: none"><li>- забезпечувати процеси моніторингу доступу до ресурсів і процесів інформаційно-телекомунікаційних систем;</li></ul>
CP12	<ul style="list-style-type: none"><li>- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;</li><li>- аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах;</li></ul>

**Мета дисципліни** – опанування основними термінами та категоріями безпеки інформації на рівні їх тлумачення та відтворення для практичного застосування та втілення у процесі діяльності майбутнього спеціаліста з кібербезпеки.

Реалізація мети вимагає трансформації програмних результатів навчання в дисциплінарні та адекватний відбір змісту навчальної дисципліни за цим критерієм.

## 2 ОЧІКУВАНІ ДИСЦИПЛІНАРНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Шифр ПРН	Дисциплінарні результати навчання (ДРН)	
	шифр ДРН	зміст
CP1	CP1-Ф14	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.
CP5	CP5-Ф14	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - проектувати та реалізовувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
CP9	CP9- Ф14	- забезпечувати функціонування системи управління інформаційною та\або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки;
CP11	CP11- Ф14	- забезпечувати процеси моніторингу доступу до ресурсів і процесів інформаційно-телекомунікаційних систем;
CP12	CP12- Ф14	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах;

## 3 БАЗОВІ ДИСЦИПЛІНИ

Назва дисципліни	Здобуті результати навчання
Ф1 Вища математика	Знати теорії та методи фундаментальних наук в об'ємі необхідному для розв'язання спеціалізованих задач та практичних проблем у галузі професійної діяльності
Ф3 Вступ до фаху	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;

#### 4 ОБСЯГ І РОЗПОДІЛ ЗА ФОРМАМИ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ ТА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Вид навчальних занять	Обсяг, години	Розподіл за формами навчання, години					
		денна		вечірня		заочна	
		аудиторні заняття	самостійна робота	аудиторні заняття	самостійна робота	аудиторні заняття	самостійна робота
лекційні	100	22	78	16	84	12	88
практичні	50	17	33	8	42	6	44
лабораторні	-	-	-	-	-	-	-
семінари	-	-	-	-	-	-	-
РАЗОМ	150	39	111	24	126	18	132

#### 5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, години самостійна робота / загальний обсяг
	<b>ЛЕКЦІЇ</b>	<b>78/100</b>
CP1-Ф14	<b>Загальні аспекти безпеки інформації.</b> Сутність та визначення термінів «безпека інформації», «інформаційна безпека», «кібербезпека». Інформаційні правовідносини. Основні нормативно-правові документи України у сфері ІБ	4/6
CP9-Ф14	<b>Основи безпеки інформаційних ресурсів.</b> Загрози безпеці інформації та інформаційних ресурсів. Загальні положення. Класифікації загроз безпеці інформації. Класифікація джерел загроз. Класифікація вразливостей безпеці. <b>Основні напрями забезпечення безпеки інформації та інформаційних ресурсів.</b> Основні визначення. Правовий захист. Організаційний захист. Інженерно-технічний захист.	16/20
CP5-Ф14	<b>Моделі безпеки інформаційних систем.</b> Теоретичні основи побудови систем безпеки. Модель дискреційного розмежування доступу. Мандатне управління доступом. Ролеве розмежування.	14/18
CP5-Ф14	<b>Криптографічні методи захисту інформації.</b> Міжнародні правила застосування шифру. Управління криптографією. Вимоги до криптографічних систем. Класифікація криптографічних методів. Проблеми та перспективи криптографічних систем. Управління ключами. Правове, організаційне та технічне забезпечення режиму електронного цифрового підпису	14/18

<b>Шифри ДРН</b>	<b>Види та тематика навчальних занять</b>	<b>Обсяг складових, години самостійна робота / загальний обсяг</b>
CP5-Ф14	<b>Загальна характеристика комплексного захисту інформації.</b> Загальні відомості, задачі КЗІ. Стратегії комплексного захисту інформації. Етапи побудови КЗІ для різних стратегій. Безпека цінних інформаційних ресурсів. Критерії цінності інформації. Виявлення та документування конфіденційних відомостей. Носії конфіденційних відомостей	8/10
CP11-Ф14	Основи інформаційного протиборства. Основні поняття інформаційного протиборства. Основи теорії інформаційної боротьби. Заходи інформаційної боротьби. Способи інформаційної боротьби. Методологія оцінки інформаційної боротьби	8/10
CP12-Ф14	<b>Нормативні документи з оцінювання захищеності інформації.</b> Розвиток стандартів безпеки. Нормативно-правова база України. Міжнародний стандарт безпеки ISO/IEC 17799. Серія стандартів ISO / IEC 27000 «Інформаційні технології. Методи забезпечення безпеки» та СУІБ ISO 27001	14/18
	<b>ПРАКТИЧНІ ЗАНЯТТЯ</b>	<b>33/50</b>
CP9-Ф14 CP11-Ф14 CP12-Ф14	Генерація випадкових та псевдовипадкових послідовностей (ВП та ПВП), а також визначення можливості їх застосування у криптографічних перетвореннях. Дослідження їх криптостійкості	15/26
CP1-Ф14 CP5-Ф14	Вирішення практично-ситуаційної задачі у сфері безпеки інформації з використанням нормативно-правової бази України та міжнародного законодавства.	18/24

## 6 ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Сертифікація досягнень студентів здійснюється за допомогою прозорих процедур, що ґрунтуються на об'єктивних критеріях відповідно до «Положення про оцінювання результатів навчання здобувачів вищої освіти».

Досягнутий рівень компетентностей відносно очікуваних, що ідентифікований під час контрольних заходів, відображає реальний результат навчання студента за дисципліною.

### 6.1 Шкали

Оцінювання навчальних досягнень студентів НТУ «ДП» здійснюється за рейтинговою (100-бальною) та інституційною шкалами. Остання необхідна (за

офіційною відсутністю національної шкали) для конвертації (переведення) оцінок мобільних студентів.

**Шкали оцінювання навчальних досягнень студентів НТУ «ДП»**

Рейтингова	Інституційна
90...100	відмінно / Excellent
74...89	добре / Good
60...73	задовільно / Satisfactory
0...59	незадовільно / Fail

Кредити навчальної дисципліни зараховується, якщо студент отримав підсумкову оцінку не менше 60-ти балів. Нижча оцінка вважається академічною заборгованістю, що підлягає ліквідації.

## 6.2 Засоби та процедури

Зміст засобів діагностики спрямовано на контроль рівня сформованості знань, умінь, комунікації, автономності та відповідальності студента за вимогами НРК до 7-го кваліфікаційного рівня під час демонстрації регламентованих робочою програмою результатів навчання.

Засоби діагностики (контрольні завдання) для поточного та підсумкового контролю дисципліни затверджуються кафедрою.

Види засобів діагностики та процедур оцінювання для поточного та підсумкового контролю дисципліни подано нижче.

### Засоби діагностики та процедури оцінювання

ПОТОЧНИЙ КОНТРОЛЬ			ПІДСУМКОВИЙ КОНТРОЛЬ	
навчальне заняття	засоби діагностики	процедури	засоби діагностики	процедури
лекції	контрольні завдання за кожною темою	виконання завдання під час лекцій	комплексна контрольна робота (ККР)	визначення середньозваженого результату поточних контролів;
практичні	контрольні завдання за кожною темою	виконання завдань під час практичних занять		виконання ККР під час заліку
	або індивідуальне завдання	виконання завдань під час самостійної роботи		

Під час поточного контролю лекційні заняття оцінюються шляхом визначення якості виконання контрольних конкретизованих завдань. Практичні заняття оцінюються якістю виконання контрольного або індивідуального завдання.

За наявності рівня результатів поточних контролів з усіх видів навчальних занять не менше 60 балів, підсумковий контроль здійснюється без участі студента шляхом визначення середньозваженого значення поточних оцінок.

Незалежно від результатів поточного контролю кожен студент під час екзамену має право виконувати ККР, яка містить завдання, що охоплюють ключові дисциплінарні результати навчання.



Кількість конкретизованих завдань ККР повинна відповідати відведеному часу на виконання. Кількість варіантів ККР має забезпечити індивідуалізацію завдання.

Значення оцінки за виконання ККР визначається середньою оцінкою складових (конкретизованих завдань) і є остаточним.

### 6.3 Критерії

Для оцінювання виконання контрольних завдань під час поточного контролю лекційних і практичних занять в якості критерія використовується коефіцієнт засвоєння, що автоматично адаптує показник оцінки до рейтингової шкали:

$$O_i = 100 a/m,$$

де  $a$  – число правильних відповідей або виконаних суттєвих операцій відповідно до еталону рішення;  $m$  – загальна кількість запитань або суттєвих операцій еталону.

Індивідуальні завдання та комплексні контрольні роботи оцінюються експертно за допомогою критеріїв, що характеризують співвідношення вимог до рівня компетентностей і показників оцінки за рейтинговою шкалою.

Зміст критеріїв спирається на компетентнісні характеристики, визначені НРК для магістерського рівня вищої освіти.

## 7. ЗАГАЛЬНІ КРИТЕРІЇ ДОСЯГНЕННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ ДЛЯ 7-го КВАЛІФІКАЦІЙНОГО РІВНЯ ЗА НРК

**Інтегральна компетентність** – здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у певній галузі професійної діяльності або у процесі навчання, що передбачає застосування певних теорій та методів відповідної науки і характеризується комплексністю та невизначеністю умов.

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
<b>Знання</b>		
<ul style="list-style-type: none"> <li>◆ концептуальні знання, набуті у процесі навчання та професійної діяльності, включаючи певні знання сучасних досягнень;</li> <li>◆ критичне осмислення основних теорій, принципів, методів і понять у навчанні та професійній</li> </ul>	- Відповідь відмінна – правильна, обґрунтована, осмислена. Характеризує наявність: - концептуальних знань; - високого ступеню володіння станом питання; - критичного осмислення основних теорій, принципів, методів і понять у навчанні та професійній діяльності	95-100
	Відповідь містить негрубі помилки або описки	90-94
	Відповідь правильна, але має певні неточності	85-89
	Відповідь правильна, але має певні неточності й недостатньо обґрунтована	80-84
	Відповідь правильна, але має певні неточності, недостатньо обґрунтована та осмислена	74-79
	Відповідь фрагментарна	70-73
	Відповідь демонструє нечіткі уявлення студента про об'єкт вивчення	65-69

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
діяльності	Рівень знань мінімально задовільний	60-64
	Рівень знань незадовільний	<60
<b>Уміння</b>		
<ul style="list-style-type: none"> <li>розв'язання складних непередбачуваних задач і проблем у спеціалізованих сферах професійної діяльності та/або навчання, що передбачає збирання та інтерпретацію інформації (даних), вибір методів та інструментальних засобів, застосування інноваційних підходів</li> </ul>	<ul style="list-style-type: none"> <li>Відповідь характеризує уміння: <ul style="list-style-type: none"> <li>виявляти проблеми;</li> <li>формулювати гіпотези;</li> <li>розв'язувати проблеми;</li> <li>обирати адекватні методи та інструментальні засоби;</li> <li>збирати та логічно й зрозуміло інтерпретувати інформацію;</li> <li>використовувати інноваційні підходи до розв'язання завдання</li> </ul> </li> </ul>	95-100
	Відповідь характеризує уміння застосовувати знання в практичній діяльності з не грубими помилками	90-94
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації однієї вимоги	85-89
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації двох вимог	80-84
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації трьох вимог	74-79
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації чотирьох вимог	70-73
	Відповідь характеризує уміння застосовувати знання в практичній діяльності при виконанні завдань за зразком	65-69
	Відповідь характеризує уміння застосовувати знання при виконанні завдань за зразком, але з неточностями	60-64
	Рівень умінь незадовільний	<60
<b>Комунікація</b>		
<ul style="list-style-type: none"> <li>донесення до фахівців і нефахівців інформації, ідей, проблем, рішень та власного досвіду в галузі професійної діяльності;</li> <li>здатність ефективно формувати комунікаційну стратегію</li> </ul>	<ul style="list-style-type: none"> <li>Вільне володіння проблематикою галузі. Зрозумілість відповіді (доповіді). Мова: - правильна; <ul style="list-style-type: none"> <li>- чиста;</li> <li>- ясна;</li> <li>- точна;</li> <li>- логічна;</li> <li>- виразна;</li> <li>- лаконічна.</li> </ul> </li> <li>Комунікаційна стратегія: <ul style="list-style-type: none"> <li>- послідовний і несуперечливий розвиток думки;</li> <li>- наявність логічних власних суджень;</li> <li>- доречна аргументації та її відповідність відстоюваним положенням;</li> </ul> </li> </ul>	95-100

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
	- правильна структура відповіді (доповіді); - правильність відповідей на запитання; - доречна техніка відповідей на запитання; - здатність робити висновки та формулювати пропозиції	
	Достатнє володіння проблематикою галузі з незначними хибами. Достатня зрозумілість відповіді (доповіді) з незначними хибами. Доречна комунікаційна стратегія з незначними хибами	90-94
	Добре володіння проблематикою галузі. Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано три вимоги)	85-89
	Добре володіння проблематикою галузі. Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано чотири вимоги)	80-84
	Добре володіння проблематикою галузі. Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано п'ять вимог)	74-79
	Задовільне володіння проблематикою галузі. Задовільна зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано сім вимог)	70-73
	Часткове володіння проблематикою галузі. Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано дев'ять вимог)	65-69
	Фрагментарне володіння проблематикою галузі. Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано 10 вимог)	60-64
	Рівень комунікації незадовільний	<60
<b>Автономність та відповідальність</b>		
<ul style="list-style-type: none"> <li>♦ управління комплексними діями або проектами, відповідальність за прийняття рішень у непередбачуваних умовах;</li> <li>♦ відповідальність за професійний розвиток окремих осіб та/або груп осіб</li> <li>♦ здатність до подальшого навчання з високим рівнем</li> </ul>	<ul style="list-style-type: none"> <li>- Відмінне володіння компетенціями менеджменту особистості, орієнтованих на:</li> <li>1) управління комплексними проектами, що передбачає: <ul style="list-style-type: none"> <li>- дослідницький характер навчальної діяльності, позначена вмінням самостійно оцінювати різноманітні життєві ситуації, явища, факти, виявляти і відстоювати особисту позицію;</li> <li>- здатність до роботи в команді;</li> <li>- контроль власних дій;</li> </ul> </li> <li>2) відповідальність за прийняття рішень в непередбачуваних умовах, що включає: <ul style="list-style-type: none"> <li>- обґрунтування власних рішень положеннями нормативної бази галузевого та державного рівнів;</li> </ul> </li> </ul>	95-100

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
автономності	- самостійність під час виконання поставлених завдань; - ініціативу в обговоренні проблем; - відповідальність за взаємовідносини; 3) відповідальність за професійний розвиток окремих осіб та/або груп осіб, що передбачає: - використання професійно-орієнтовних навичок; - використання доказів із самостійною і правильною аргументацією; - володіння всіма видами навчальної діяльності; 4) здатність до подальшого навчання з високим рівнем автономності, що передбачає: - ступінь володіння фундаментальними знаннями; - самостійність оцінних суджень; - високий рівень сформованості загальнонавчальних умінь і навичок; - самостійний пошук та аналіз джерел інформації	
	Упевнене володіння компетенціями менеджменту особистості (не реалізовано дві вимоги)	90-94
	Добре володіння компетенціями менеджменту особистості (не реалізовано три вимоги)	85-89
	Добре володіння компетенціями менеджменту особистості (не реалізовано чотири вимоги)	80-84
	Добре володіння компетенціями менеджменту особистості (не реалізовано шість вимог)	74-79
	Задовільне володіння компетенціями менеджменту особистості (не реалізовано сім вимог)	70-73
	Задовільне володіння компетенціями менеджменту особистості (не реалізовано вісім вимог)	65-69
	Рівень автономності та відповідальності фрагментарний	60-64
	Рівень автономності та відповідальності незадовільний	<60

## 8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

### 8.1. Основні

1. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем/ М.В.Гайворонський, О.М. Новіков.–К.: Видавнича група BVH, 2009. –608 с., іл
2. Юдін О.К., Конахович Г.Ф., Корченко О.Г., Захист інформації в мережах передачі даних: підручник/О.К. Юдін, Г.Ф.Конахович, О.Г.Корченко. –К.:Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. –714с., іл.
3. .Богуш В.М., Довидьков О.А. Основи захищених інформаційних технологій/ В.М.Богуш, О.А.Довидьков. –К.: ДУІКТ, 2005. –450 с.

### 8.2. Допоміжні

1. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. –К.: МК-Прес, 2005.–432 с.
2. Бурячок В.Л. Інформаційна та кібербезпека / В.Л.Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. –К.: ДУТ, 2015. –288 с.

3. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / С.М. Головань, С.Б. Гордієнко, О.С. Петров, В.О. Хорошко, Л.М. Щербак; під ред. В.О. Хорошко.—Луганськ: Ноулідж, 2012.—480 с

### **8.3. Інформаційні ресурси**

1. <https://zakon.rada.gov.ua>

Навчальне видання

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ  
«Основи забезпечення безпеки інформації» для бакалаврів  
спеціальності 125 «Кібербезпека»

Розробник: Мілінчук Юлія Анатоліївна