

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

Кафедра безпеки інформації та телекомунікацій

«ЗАТВЕРДЖЕНО»
на засіданні кафедри БІТ

(протокол № 9 від 23.04.2019 р.)

завідувач кафедри
Корнієнко В.І. _____

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Системи управління інформаційною безпекою»

Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітній рівень.....	магістр
Освітньо-професійна програма	Кібербезпека
Спеціалізація	
Статус	нормативна
Загальний обсяг	5 кредитів ЄКТС (150 годин)
Форма підсумкового контролю	екзамен
Термін викладання	1-й семестр
Мова викладання	українська

Викладачі: ст. в. Тимофєєв Д.С.

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 «Системи управління інформаційною безпекою» для магістрів спеціальності 125 «Кібербезпека» / Нац. техн. ун-т. «Дніпровська політехніка», каф. безпеки інформації та телекомунікацій – Д. : НТУ «ДП», 2019. – 13 с.

Розробник – Тимофєєв Д.С.

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.

Робоча програма буде в пригоді для формування змісту підвищення кваліфікації науково-педагогічних працівників кафедр університету.

Погоджено рішенням методичної комісії спеціальності 125 «Кібербезпека» (протокол № 9 від 23.04.2019 р.).

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	7
6.1 Шкали	7
6.2 Засоби та процедури.....	7
6.3 Критерії.....	9
7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ	12
8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ.....	12

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 ФЗ «Системи управління інформаційною безпекою» віднесено такі результати навчання:

CP1	Використовувати управлінсько-організаційні та правові методи, засоби й заходи для реалізації проектних рішень з побудови систем забезпечення інформаційної та кібернетичної безпеки.
CP2	Проводити системні дослідження та застосовувати їх в керуванні проектами для забезпечення інформаційної та кібербезпеки.
CP3	Використовувати математичні, технічні та правові методи забезпечення інформаційної та кібернетичної безпеки
ЗР3	Превентивно і аварійно планувати, управляти заходами безпеки професійної діяльності, приймати рішення у складних та непередбачуваних ситуаціях, лідерські якості на посаді керівника
ЗР4	Письмова й усна комунікації українською та іноземною мовами
ЗР6	Вмотивованість щодо подальшого навчання з високим рівнем автономності.

Мета дисципліни – формування компетентностей щодо впровадження, підтримки та модернізації систем управління інформаційною безпекою.

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-ФЗ	Використовувати управлінсько-організаційні та правові методи, засоби й заходи для реалізації проектних рішень з побудови систем забезпечення інформаційної та кібернетичної безпеки.
CP2	CP2-ФЗ	Проводити системні дослідження та застосовувати їх в керуванні проектами для забезпечення інформаційної та кібербезпеки.
CP3	CP3-ФЗ	Використовувати математичні, технічні та правові методи забезпечення інформаційної та кібернетичної безпеки
ЗР3	ЗР3-ФЗ	Превентивно і аварійно планувати, управляти заходами безпеки професійної діяльності, приймати рішення у складних та непередбачуваних ситуаціях, лідерські якості на посаді керівника
ЗР4	ЗР4-ФЗ	Письмова й усна комунікації українською та іноземною мовами
ЗР6	ЗР6-ФЗ	Вмотивованість щодо подальшого навчання з високим рівнем автономності.

3 БАЗОВІ ДИСЦИПЛІНИ

Назва дисципліни	Здобуті результати навчання
Фахові дисципліни освітньої програми ступеня бакалавра	результати навчання за ОП бакалавра спеціальності 125

Назва дисципліни	Здобуті результати навчання
спеціальності 125 Кібербезпека	

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	120	60	60	30	90	16	104
практичні	30	14	16	8	22	4	26
лабораторні	-	-	-	-	-	-	-
семінари	-	-	-	-	-	-	-
РАЗОМ	150	74	76	38	112	20	130

5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, години
	ЛЕКЦІЇ	120
CP1-Ф3 ЗР6-Ф3	1 Характеристика та обрання основних підходів до управління інформаційною безпекою 1. Базова термінологія 1.1. Система 1.2. Системний підхід 1.3. Процес 1.4. Процесний підхід 1.5. Управління 1.6. Циклічна модель поліпшення процесів 1.7. Системний підхід до управління організацією 1.8. Процесний підхід до управління організацією 1.9. Інформаційна безпека	20
CP1-Ф3 ЗР4-Ф3	2 Аналіз та застосування основних стандартів з систем і процесів управління інформаційною безпекою 2. Стандартизація систем і процесів управління інформаційною безпекою 2.1. Серія стандартів ISO / IEC 27000 «Інформаційні технології. Методи забезпечення безпеки» 2.1.1. ISO / IEC 27000- СУІБ: визначення та основні принципи 2.1.2. ISO / IEC 27001 вимоги до СУІБ 2.1.3. ISO / IEC 27002 практичні правила управління ІБ 2.1.4. ISO / IEC 27003 посібник з впровадження СУІБ 2.1.5. ISO / IEC 27004 оцінка функціонування СУІБ 2.1.6. ISO / IEC 27005 управління ризиками ІБ 2.1.9. ISO / IEC 27011 посібник з управління ІБ для телекомунікаційних компаній на основі ISO / IEC 27002	30

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, години
	2.1.10. ISO / IEC 27013 - керівництво з інтегрованого впровадження стандартів ISO / IEC 20000 і 27001 2.1.11. ISO / IEC 27014 - інфраструктура керівництва ІБ 2.1.12. ISO / IEC 27015 - керівництво з управління ІБ для фінансових сервісів 2.1.13. ISO / IEC 27031: 2011 - керівництво по готовності інформаційних і телекомунікаційних технологій для забезпечення безперервності бізнесу 2.1.14. ISO / IEC 27033 - управління безпекою мереж 2.1.15. ISO / IEC 27035: 2011-управління інцидентами ІБ 2.1.16. ISO / IEC 27037- керівництво по ідентифікації, збору та / або отриманню і забезпеченню збереження свідчень, представлених в електронній формі 2.2. Стандарти на окремі процеси управління ІБ і оцінку безпеки ІТ 2.2.1. ISO / IEC 13335 - методи і засоби забезпечення безпеки інформаційних технологій 2.2.2. ISO / IEC 15408 та ISO / IEC 18045 - загальні критерії та методології оцінки безпеки інформаційних технологій	
CP2-Ф3 ЗР4-Ф3	3 Розробка та аналіз політики інформаційної безпеки 3. Політика інформаційної безпеки 3.1. Поняття політики забезпечення ІБ і політики ІБ організації 3.2. Причини розробки політики ІБ 3.3. Основні вимоги та принципи, що враховуються при розробці та впровадженні політики ІБ 3.4. Зміст політики ІБ 3.4.1. Зміст корпоративної політики ІБ 3.4.2. Зміст приватних політик ІБ 3.5. Життєвий цикл політики ІБ 3.5.1. Розробка політики ІБ 3.5.2. Впровадження політики ІБ 3.5.3. Застосування політики ІБ 3.5.4. Анулювання політики ІБ 3.6. Відповідальність за виконання політики ІБ	30
CP3-Ф3 ЗР6-Ф3	4 Запровадження управління ІБ із застосуванням СУІБ 4. Управління і система управління інформаційною безпекою 4.1. Необхідність управління забезпеченням ІБ організації 4.2. Діяльність по забезпеченню ІБ організації як процес 4.3. Визначення управління ІБ організації 4.4. Управління ІБ інформаційно-телекомунікаційних технологій організації 4.5. Система управління ІБ організації 4.5.1. Область дії СУІБ 4.5.2. Документальне забезпечення СУІБ 4.5.3. Політика СУІБ 4.5.4. Підтримка СУІБ з боку керівництва	40
	ПРАКТИЧНІ ЗАНЯТТЯ	30
CP1-CP3- Ф3	Розробка проекту реалізації СУІБ Дослідження реальних об'єктів інформаційної діяльності	30

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, години
ЗР3-Ф3, ЗР4-Ф3, ЗР6-Ф3	Інвентаризація та класифікація інформаційних активів Програмне моделювання процесу управління ризиками інформаційної безпеки	
РАЗОМ		150

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 8-го кваліфікаційного рівня під час демонстрації регламентованих робочою програмою результатів навчання.

Студент на контрольних заходах має виконувати завдання, орієнтовані виключно на демонстрацію дисциплінарних результатів навчання (розділ 2).

Засоби діагностики, що надаються студентам на контрольних заходах у вигляді завдань для поточного та підсумкового контролю, формуються шляхом конкретизації вихідних даних та способу демонстрації дисциплінарних 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; виконання ККР під час екзамену за бажанням студента
практичні	контрольні завдання за кожною темою	виконання завдань під час практичних занять		
	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.

Якщо зміст певного виду занять підпорядковано декільком дескрипторам, то інтегральне значення оцінки може визначатися з урахуванням вагових коефіцієнтів, що встановлюються викладачем.

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.

Інтегральне значення оцінки виконання ККР може визначатися з урахуванням вагових коефіцієнтів, що встановлюється кафедрою для кожного дескриптора НРК.

6.3 Критерії

Реальні результати навчання студента ідентифікуються та вимірюються відносно очікуваних під час контрольних заходів за допомогою критеріїв, що описують дії студента для демонстрації досягнення результатів навчання.

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 (подано нижче).

**Загальні критерії досягнення результатів навчання
для 8-го кваліфікаційного рівня за НРК**

Інтегральна компетентність – здатність розв'язувати складні задачі і проблеми у певній галузі професійної діяльності або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
Знання		
<ul style="list-style-type: none"> ♦ спеціалізовані концептуальні знання, набуті у процесі навчання та/або професійної діяльності на рівні новітніх досягнень, які є основою для оригінального мислення та інноваційної діяльності, зокрема в контексті дослідницької роботи; ♦ критичне осмислення проблем у навчанні та /або професійній діяльності та на межі предметних галузей 	Відповідь відмінна – правильна, обґрунтована, осмислена. Характеризує наявність: <ul style="list-style-type: none"> - спеціалізованих концептуальних знань на рівні новітніх досягнень; - критичне осмислення проблем у навчанні та/або професійній діяльності та на межі предметних галузей 	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
	Рівень знань мінімально задовільний	60-64
	Рівень знань незадовільний	<60
Уміння		

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
<ul style="list-style-type: none"> ♦ розв'язання складних задач і проблем, що потребує оновлення та інтеграції знань, часто в умовах неповної/недостатньої інформації та суперечливих вимог; ♦ провадження дослідницької та/або інноваційної діяльності 	Відповідь характеризує уміння: <ul style="list-style-type: none"> - виявляти проблеми; - формулювати гіпотези; - розв'язувати проблеми; - оновлювати знання; - інтегрувати знання; - провадити інноваційну діяльність; - провадити наукову діяльність 	95-100
	Відповідь характеризує уміння застосовувати знання в практичній діяльності з негрубими 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		
Комунікація		
<ul style="list-style-type: none"> ♦ зрозуміле і недвозначне донесення власних висновків, а також знань та пояснень, що їх обґрунтовують, до фахівців і нефахівців, зокрема до осіб, які навчаються; ♦ використання іноземних мов у професійній діяльності 	Зрозумілість відповіді (доповіді). Мова: <ul style="list-style-type: none"> - правильна; - чиста; - ясна; - точна; - логічна; - виразна; - лаконічна. Комунікаційна стратегія: <ul style="list-style-type: none"> - послідовний і несуперечливий розвиток думки; - наявність логічних власних суджень; - доречна аргументації та її відповідність відстоюваним положенням; - правильна структура відповіді (доповіді); - правильність відповідей на запитання; - доречна техніка відповідей на запитання; - здатність робити висновки та формулювати пропозиції; 	95-100

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
	- використання іноземних мов у професійній діяльності	
	Достатня зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія з незначними хибами	90-94
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано три вимоги)	85-89
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано чотири вимоги)	80-84
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано п'ять вимог)	74-79
	Задовільна зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано сім вимог)	70-73
	Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано дев'ять вимог)	65-69
	Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано 10 вимог)	60-64
	Рівень комунікації незадовільний	<60
Автономність та відповідальність		
<ul style="list-style-type: none"> ♦ відповідальність за розвиток професійного знання і практик, оцінку стратегічного розвитку команди; ♦ здатність до подальшого навчання, яке значною мірою є автономним та самостійним 	Відмінне володіння компетенціями: <ul style="list-style-type: none"> - використання принципів та методів організації діяльності команди; - ефективний розподіл повноважень в структурі команди; - підтримка врівноважених стосунків з членами команди (відповідальність за взаємовідносини); - стресовитривалість; - саморегуляція; - трудова активність в екстремальних ситуаціях; - високий рівень особистого ставлення до справи; - володіння всіма видами навчальної діяльності; - належний рівень фундаментальних знань; - належний рівень сформованості загальнонавчальних умінь і навичок 	95-100
	Упевнене володіння компетенціями автономності та відповідальності з незначними хибами	90-94
	Добре володіння компетенціями автономності та відповідальності (не реалізовано дві вимоги)	85-89
	Добре володіння компетенціями автономності та відповідальності (не реалізовано три вимоги)	80-84
	Добре володіння компетенціями автономності та відповідальності (не реалізовано чотири вимоги)	74-79
	Задовільне володіння компетенціями автономності та відповідальності (не реалізовано п'ять вимог)	70-73

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
	Задовільне володіння компетенціями автономності та відповідальності (не реалізовано шість вимог)	65-69
	Задовільне володіння компетенціями автономності та відповідальності (рівень фрагментарний)	60-64
	Рівень автономності та відповідальності незадовільний	<60

7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Технічні засоби навчання.

Дистанційна платформа Moodle.

8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Грайворонський М.В., Новіков О.М Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BVH, 2009. – 608 с.
2. А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой Основы управления информационной безопасностью. Учебное пособие для вузов. - 2-е изд., испр. - М.: Горячая линия-Телеком, 2014. -244 с.: ил. - Серия «Вопросы управления информационной безопасностью. Выпуск 1»
3. Тимофеев Д.С. Методичні рекомендації до самостійної роботи студентів з дисципліни «Системи управління інформаційною безпекою»/ Д.С. Тимофеев [та ін.]; Нац. гірн. ун-т, каф. безпеки інформації та телекомунікацій. – Д. : НГУ, 2016. – 90 с.
4. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).
5. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).
6. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT)

Навчальне видання

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Системи управління інформаційною безпекою» для магістрів
спеціальності 125 «Кібербезпека»

Розробник: Дмитро Сергійович Тимофєєв