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 БІТ
Корнієнко В.І. _____

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Комплексні системи захисту інформації»

Галузь знань ……..…	12 Інформаційні технології
Спеціальність ……...	125 Кібербезпека
Освітній рівень…….	бакалавр
Освітньо-професійна програма	Кібербезпека
Спеціалізація ……	
Статус ……	нормативна
Загальний обсяг ..…….	9 кредитів ЄКТС (270 годин)
Форма підсумкового контролю	екзамен
Термін викладання ……..	8-й семестр
Мова викладання …….	українська

Викладач: ст. викладач Кручінін О.В.

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 «Комплексні системи захисту інформації» для бакалаврів спеціальності 125 «Кібербезпека» / Нац. техн. ун-т. «Дніпровська політехніка», каф. безп. інф. та телеком. – Д.: НТУ «ДП», 2019. – 8 с.

Розробник – Кручінін О.В.

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 № 8 від 23.04.2019).

ЗМІСТ

1 МЕТА НАВЧАЛЬНОЇ ДИЦИПЛІНИ

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 Ф9 «Комплексні системи захисту інформації» віднесено такі результати навчання:

СР1	- розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем;
СР5	- проектувати та реалізувати 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;
СР7	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання та ін.) наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - вирішувати задачі експертизи, випробування комплексних систем захисту інформації

Мета дисципліни – формування у студентів компетентності щодо призначення комплексних систем захисту інформації (КСЗІ), методики створення КСЗІ, методик випробувань КСЗІ та вимог з експлуатації КСЗІ

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**
СР1	СР1-Ф9	- розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем;;
СР5	СР5-Ф9	- проектувати та реалізувати 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;
СР7	СР7-Ф9	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до

Шифр ПРН	Дисциплінарні результати навчання (ДРН)	
	шифр ДРН	зміст
		ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання та ін.) наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - вирішувати задачі експертизи, випробування комплексних систем захисту інформації

3 БАЗОВІ ДИСЦИПЛІНИ

Назва дисципліни	Здобуті результати навчання
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; - адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; - використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
Ф8 Мережеві технології і протоколи Ф11 Операційні системи	- здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; - розробляти та аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; - застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем; - здійснювати захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші), а також встановлених режимів безпечного функціонування інформаційно-телекомунікаційних системах; - виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної і\або кібербезпеки в інформаційнотелекомунікаційних системах. - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

Назва дисципліни	Здобуті результати навчання
	- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); - вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

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	135	52	83			14	121
практичні	135	52	83			12	123
лабораторні	-	-	-			-	-
семінари	-	-	-			-	-
РАЗОМ	270	104	166			26	244

5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Шифри ДРН	**Види та тематика навчальних занять**	**Обсяг складових,** *години*
	ЛЕКЦІЇ	**135**
СР1-Ф9 СР5-Ф9	**1. Проектування комплексної системи захисту інформації**	72
	1.1. Основні положення законодавчих, нормативно-правових та нормативних документів. Терміни та визначення.	
	1.2. Обґрунтування необхідності створення КСЗІ в АС	
	1.3. Обстеження середовищ функціонування АС	
	1.4. Модель загроз та модель порушника	
	1.5. Політика безпеки інформації в ІТС	
	1.6. Розробка технічного завдання на створення АС	
	1.6. Розробка проекту КСЗІ	
СР5-Ф9 СР7-Ф9	**2. Випробування та впровадження комплексної системи захисту інформації**	42
	2.1 Введення КСЗІ в дію	
	2.2 Попередні випробування КСЗІ	
	2.3 Дослідна експлуатація КСЗІ	
	2.4 Державна експертиза КСЗІ	
СР7-Ф9	**3. Супровід комплексної системи захисту інформації**	21
	3.1 Функції служби захисту інформації при експлуатації КСЗІ в ІТС	

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, *години*
	3.2 Експлуатаційні документи для КСЗІ в ІТС	
	ПРАКТИЧНІ ЗАНЯТТЯ	**135**
СР1-Ф9 СР5-Ф9	**1. 1. Проектування комплексної системи захисту інформації**	68
	1.1 Визначення критеріїв захищеності для АС	
	1.2 Обстеження середовищ функціонування АС.	
	1.3 Розробка моделі загроз та моделі порушника	
	1.4 Розробка технічного завдання на створення КСЗІ	
СР5-Ф9 СР7-Ф9	**2 Випробування та впровадження комплексної системи захисту інформації**	48
	2.1 Інсталяція КЗЗ «Гриф-4» для АС класу «1»	
	2.2 Інсталяція КЗЗ «Гриф-4» для АС класу «2»	
	2.3 Основні захисні механізми операційних систем	
	2.4 Розробка декларації відповідності КСЗІ АС	
СР7-Ф9	**3 Супровід комплексної системи захисту інформації**	19
	3.1 Розробка положення СЗІ	
	3.2 Розробка експлуатаційні документи для КСЗІ в ІТС	
	РАЗОМ	**270**

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

<table>
<tr><th colspan="3">ПОТОЧНИЙ КОНТРОЛЬ</th><th colspan="2">ПІДСУМКОВИЙ КОНТРОЛЬ</th></tr>
<tr><th>навчальне заняття</th><th>засоби діагностики</th><th>процедури</th><th>засоби діагностики</th><th>процедури</th></tr>
<tr><td>лекції</td><td>контрольні завдання за кожною темою</td><td>виконання завдання під час лекцій</td><td rowspan="3">комплексна контрольна робота (ККР)</td><td rowspan="3">визначення середньозваженого результату поточних контролів;

виконання ККР під час екзамену</td></tr>
<tr><td>практичні</td><td>контрольні завдання за кожною темою</td><td>виконання завдань під час практичних занять</td></tr>
<tr><td></td><td>або індивідуальне завдання</td><td>виконання завдань під час самостійної роботи</td></tr>
</table>

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 *а* – 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 бакалаврського рівня вищої освіти.

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**
	Знання	
♦ концептуальні знання, набуті у процесі навчання та професійної діяльності, включаючи певні знання сучасних досягнень; ♦ критичне осмислення основних теорій, принципів, методів і понять у навчанні та професійній діяльності	- 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
	Рівень знань мінімально задовільний	60-64
	Рівень знань незадовільний	<60
	Уміння	
♦ розв'язання складних непередбачуваних задач і проблем у спеціалізованих сферах професійної діяльності та/або навчання, що	- Відповідь характеризує уміння: - виявляти проблеми; - формулювати гіпотези; - розв'язувати проблеми; - обирати адекватні методи та інструментальні засоби; - збирати та логічно й зрозуміло інтерпретувати інформацію; - використовувати інноваційні підходи до розв’язання завдання	95-100
	Відповідь характеризує уміння застосовувати знання в	90-94

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
передбачає збирання та інтерпретацію інформації (даних), вибір методів та інструментальних засобів, застосування інноваційних підходів	практичній діяльності з не грубими помилками	
	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
Комунікація		
♦ донесення до фахівців і нефахівців інформації, ідей, проблем, рішень та власного досвіду в галузі професійної діяльності; ♦ здатність ефективно формувати комунікаційну стратегію	- Вільне володіння проблематикою галузі. Зрозумілість відповіді (доповіді). Мова: - правильна; - - чиста; - - ясна; - - точна; - - логічна; - - виразна; - - лаконічна. Комунікаційна стратегія: - 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
	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	85-89

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
	комунікаційна стратегія (сумарно не реалізовано три вимоги)	
	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
Автономність та відповідальність		
♦ управління комплексними діями або проектами, відповідальність за прийняття рішень у непередбачуваних умовах; ♦ відповідальність за професійний розвиток окремих осіб та/або груп осіб ♦ здатність до подальшого навчання з високим рівнем	- Відмінне володіння компетенціями менеджменту особистості, орієнтованих на: 1) управління комплексними проектами, що передбачає: - дослідницький характер навчальної діяльності, позначена вмінням самостійно оцінювати різноманітні життєві ситуації, явища, факти, виявляти і відстоювати особисту позицію; - здатність до роботи в команді; - контроль власних дій; 2) відповідальність за прийняття рішень в непередбачуваних умовах, що включає: - обґрунтування власних рішень положеннями нормативної бази галузевого та державного рівнів; - 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;	95-100

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
автономності	- 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

7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Система дистанційного навчання НТУ ДП
Комплекс засобів захисту «Гриф-3»
Комплекс засобів захисту «Гриф-4»
Комплекс засобів захисту «BBOS»
Комплекс засобів захисту «Лоза-1»

8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

8.1. Основні

1. Грайворонський М.В., Новіков О.М Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

2. 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.
3. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – Наука и техника, Санкт-Петербург, 2004. – 384 с.
4. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. Пособие для ВУЗов. – М: Горячая линия – Телеком, 2004 – 280 с.
5. Гребенніков В. Комплексні системи захисту інформації. Проектування, впровадження, супровід / В. Гребенніков — «Издательские решения»

8.2. Нормативна

1. Закон України „Про Державну службу спеціального зв'язку та захисту інформації України".
2. Закон України „Про інформацію".
3. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах".
4. Закон України „Про основні засади державного нагляду (контролю) у сфері господарської діяльності".
5. Закон України „Про наукову і науково-технічну експертизу".
6. Положення про технічний захист інформації в Україні. Указ Президента України від 27.09.1999 № 1229.
7. Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України. Указ Президента України від 30.06.2011 № 717/2011.
8. Концепція технічного захисту інформації в Україні. Постанова КМ України від 08.10.1997 № 1126.
9. Про деякі питання захисту інформації, охорона якої забезпечується державою. Постанова КМ України від 13.03.2002 № 281.
10. Положення про державний контроль за станом технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 87, зареєстрований в Міністерстві юстиції України 10.07.2007 за № 785/14052.
11. Перелік обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних. Постанова КМ України від 04.02.1998 № 121.
12. Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. Постанова КМ України від 16.02.1998 № 180.
13. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах. Постанова КМ України від 16.11.2002 № 1772.
14. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова КМ України від 29.03.2006 № 373.
15. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
16. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
17. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
18. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.
19. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.

20. ДБН 2.2-3-2004 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.
21. ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.
22. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
23. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
24. ГОСТ 34.936-91 Информационная технология. Локальные вычислительные сети. Определение услуг уровня управления доступом к среде.
25. ГОСТ 28195-89 Оценка качества программных средств. Общие положения.
26. РД 50-34.698-90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов.
27. РД 50-682-89 50-682-89 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения.
28. Комплекс стандартов Единая система программной документации (ЕСПД).
29. Комплекс стандартов Единая система конструкторской документации (ЕСКД).
30. ДСТУ 1.5:2003 Правила побудови, викладання, оформлення та вимоги до змісту нормативних документів.
31. НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.
32. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
33. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
34. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 04.12.2000 № 53.
35. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці”, затверджене наказом Адміністрації Держспецзв'язку від 15.04.2013 № 215
36. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
37. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
38. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
39. 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, затверджений наказом ДСТСЗІ СБ України від 20.12.2000 № 60.

40. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
41. НД ТЗІ 2.5-008-2002 Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2, затверджений наказом ДСТСЗІ СБ України від 13.12.2002 № 84.
42. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 02.04.2003 № 33.
43. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ-95), затверджені наказом Державної служби України з питань технічного захисту інформації від 09.06.1995 № 25.
44. НД ТЗІ 2.7-011-2012 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв.
45. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ-ПЕМВН-95), затверджені наказом Державної служби України з питань технічного захисту інформації від 09.06.1995 № 25.
46. Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від 26.03.2007 № 45, зареєстрований в Міністерстві юстиції України 10.04.2007 за № 320/13587.
47. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Наказ Адміністрації Держспецзв'язку від 02.12.2014 № 660 зареєстрований в Міністерстві юстиції Україні т28 січня 2015 р. за № 90/26535.
48. Положення про державну експертизу в сфері технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від16.05.2007 № 93, зареєстрований в Міністерстві юстиції України 16.07.2007 за № 820/14087 із змінами, затвердженими наказом Адміністрації Держспецзв'язку від 10.10.2012 № 567, зареєстрованим в Міністерстві юстиції України 06.11.2012 за № 1863/22175.
49. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб, затверджене наказом ДСТСЗІ СБ України від 23.02.2002 № 9, зареєстрованим в Міністерстві юстиції України 13.03.2002 за № 245/6533.
50. Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України. Постанова КМ України від від 16 листопада 2016 р. № 821
51. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб. Наказ ДСТСЗІ СБ України від 23.02.2002 № 9, зареєстрований в Міністерстві юстиції України 13.03.2002 за №245/6533.
52. Ліцензійні умови провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України Затверджена Постановою КМ України від від 16 листопада 2016 р. № 821
53. 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.
54. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

55. НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.
56. Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію. Постанова КМ України від 19 жовтня 2016 р. № 736.

8.3. Допоміжні

1. . Г. Ф. Конахович Захист інформації в телекомунікаційних системах , – МК-Пресс, 2005. – 288 с.
2. О. К. Юдін, О.Г. Корченко, Г.Ф. Конахович Захист інформації в мережах передачі даних , – ТИД Інтерсервіс, 2009.
3. В. В. Домарев Безопасность информационных технологий. Методология создания систем защиты, – ТИД "ДС", 2002. – 688 с.
4. М.С. Вертузаєв Захист інформації в комп'ютерних системах від несанкціонованого доступу/ М. С. Вертузаєв, О. М. Юрченко. – К.: Вид-во Європейського університету, 2001. – 322 с.
5. І.Д. Горбенко Захист інформації в інформаційно-телекомунікаційних системах/І. Д. Горбенко, Т. О. Гріненко. – Х.: ХНУРЕ, 2004. – 368 с.

8.4. Інформаційні ресурси

1. Державна служба спеціального зв’язку та захисту інформації України. – Спосіб доступу: URL: dssszi.gov.ua. – Нормативні документи
2. Верховна Рада України. – Спосіб доступу: URL: rada.gov.ua. – Нормативні документиДержавна служба спеціального зв’язку та захисту інформації України. – Спосіб доступу: URL: dssszi.gov.ua. – Нормативні документи.

Навчальне видання

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Комплексні системи захисту інформації» для бакалаврів
спеціальності 125 «Кібербезпека»

Розробник –Кручінін О.В.