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

Кафедра безпеки інформації та телекомунікацій

«ЗАТВЕРДЖЕНО»
Завідувач кафедри
_____ Корнієнко В.І.
«20» 05 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Кіберзахист»

Галузь знань ……..…	12Інформаційні технології
Спеціальність ……...	125 Кібербезпека
Освітній рівень…….	бакалавр
Освітньо-професійна програма	Кібербезпека
Спеціалізація ……	Кібербезпека
Статус ……	
Загальний обсяг ..…….	10 кредити ЄКТС (300 годин)
Форма підсумкового контролю	екзамен
Термін викладання ……..	7, 8-й семестри
Мова викладання …….	українська

Викладачі: ст.викл. Мєшков В.І.

Пролонговано: на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

Дніпро
2022

Робоча програма навчальної дисципліни «**Кіберзахист**» для бакалаврівза освітньо-професійною програмою«Кібербезпека» / Нац. техн. ун-т. «Дніпровська політехніка», каф. безп. інф. та телеком. – Д.: НТУ «ДП», 2022. – 16 с.

Розробник – Мєшков Вадим Ігорович

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 № 6 від 20.05.2022).

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 Ф6 «Кіберзахист» віднесено такі результати навчання:

СР1	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \абокібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.
СР2	- 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\абокібербезпеки в інформаційнотелекомунікаційних системах.
СР3	- забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на комплексів засобів захисту.
СР4	- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - 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.

Мета дисципліни–опанувати сучасні методи і моделі інформаційної безпеки та/або 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
СР1	СР1-Ф6	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \абокібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.
СР2	СР2-Ф6	- 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\абокібербезпеки в інформаційнотелекомунікаційних системах.
СР3	СР3-Ф6	- забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на комплексів засобів захисту.
СР4	СР4-Ф6	- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

Шифр ПРН	Дисциплінарні результати навчання (ДРН)	
	шифр ДРН	зміст
		- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - 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.

3 БАЗОВІ ДИСЦИПЛІНИ

Назва дисципліни	Здобуті результати навчання
Основи забезпечення безпеки інформації	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \абокібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.
Інформаційні технології Мережеві технології і протоколи Архітектура комп'ютерів 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\абокібербезпеки в інформаційнотелекомунікаційних системах.
Програмування і алгоритмічні мови	- забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом

Назва дисципліни	Здобуті результати навчання
Прикладна криптологія	встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на комплексів засобів захисту.
Мережеві технології і протоколи	- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - 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	78	78	123				
практичні	59	59	100				
лабораторні							
семінари							
РАЗОМ	360	137	223				

5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Шифри ДРН	**Види та тематика навчальних занять**	**Обсяг складових,** *години Ауд./Сам.*
	ЛЕКЦІЇ	**78 / 123**
СР1-Ф6	1.1 Нормативні акти і документизабезпечення встановленої політики інформаційної безпеки і \абокібербезпеки. 1.2 Розробка проектної документації, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем. 1.3 Виконання аналізу реалізації прийнятої політики інформаційної і /або кібербезпеки.	20 / 32
СР2-Ф6	2.1 Розробка та аналіз проекту інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. 2.2 Структура сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем. 2.3 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. 2.4 Аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної і\абокібербезпеки в інформаційнотелекомунікаційних системах.	20 / 31
СР3-Ф6	3.1 Забезпечення процесу захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту. 3.2 Забезпечення функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. 3.3 Розробка експлуатаційної документації на комплексів засобів захисту.	19 / 30
СР4-Ф6	4.1 Задачі супроводу (огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. 4.2Заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. 4.3Задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). 4.4Задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.	19 / 30

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, *години Ауд./Сам.*
	ЛАБОРАТОРНІ ЗАНЯТТЯ	**59 / 100**
СР1-Ф6	Розробка проектної документації, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем.	16 / 25
СР2-Ф6	Розробка та аналіз проекту інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. Структура сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем. Аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної і\абокібербезпеки в інформаційнотелекомунікаційних системах.	15 / 25
СР3-Ф6	Розробка експлуатаційної документації на комплексів засобів захисту.	14 / 25
СР4-Ф6	Системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. Заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. Управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).	14 / 25
	РАЗОМ	**360**

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.

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 rowspan="2">практичні</td><td>контрольні завдання за кожною темою</td><td>виконання завдань під час практичних занять</td></tr>
<tr><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 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 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Технічні засоби навчання.

8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

8.1. Основні

1. Грайворонський М.В., Новіков О.М Безпека інформаційно-комунікаційних систем. –
2. Гребенніков В. Комплексні системи захисту інформації. Проектування, впровадження, супровід / В. Гребенніков — «Издательскиерешения»

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 Информационнаятехнология. Комплекс стандартов на автоматизированныесистемы. Виды, комплектность и обозначениедокументов при созданииавтоматизированных систем.
22. ГОСТ 34.601-90 Информационнаятехнология. Комплекс стандартов на автоматизированныесистемы. Автоматизированныесистемы. Стадиисоздания.
23. ГОСТ 34.602-89 Информационнаятехнология. Комплекс стандартов на автоматизированныесистемы. Техническоезадание на созданиеавтоматизированнойсистемы.
24. ГОСТ 34.936-91 Информационнаятехнология. Локальныевычислительные сети. Определение услуг уровняуправления доступом к среде.
25. ГОСТ 28195-89 Оценкакачествапрограммныхсредств. Общиеположения.
26. РД 50-34.698-90 Методическиеуказания. Информационнаятехнология. Комплекс стандартов и руководящихдокументов на автоматизированныесистемы. Требования к содержаниюдокументов.
27. РД 50-682-89 50-682-89 Методическиеуказания. Информационнаятехнология. Комплекс стандартов и руководящихдокументов на автоматизированныесистемы. Общиеположения.
28. Комплекс стандартовЕдиная система программнойдокументации (ЕСПД).
29. Комплекс стандартовЕдиная система конструкторскойдокументации (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. ДомаревБезопасностьинформационныхтехнологий. Методологиясоздания 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
«Кіберзахист» для бакалаврів
спеціальності 125 «Кібербезпека»

Розробник: Мєшков Вадим Ігорович