Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра безпеки інформаційних систем і технологій

“ЗАТВЕРДЖУЮ”

Проректор з науково-педагогічної роботи

_____ Антон ПАНТЕЛЕЙМОНОВ

“___” _____ 2020 р.

Робоча програма навчальної дисципліни

Системи технічного захисту інформації

рівень вищої освіти __перший (бакалаврський)__

галузь знань 12 «Інформаційні технології»

спеціальність 125 – «Кібербезпека»

освітня програма Кібербезпека

спеціалізація

вид дисципліни ___обов’язкова__

факультет комп’ютерних наук

2020 / 2021 навчальний рік

2

Програму рекомендовано до затвердження вченою радою факультету (інституту, центру)

"31" серпня 2020 року, протокол № 12

РОЗРОБНИКИ ПРОГРАМИ: Громико Ігор Олексійович, кандидат технічних наук, доцент, професор кафедри безпеки інформаційних систем і технологій.

Програму схвалено на засіданні кафедри безпеки інформаційних систем і технологій

Протокол від "31" серпня 2020 року № 1

Завідувач кафедри безпеки інформаційних систем і технологій

_____ Рассомахін С.Г.
(підпис) (прізвище та ініціали)

Програму погоджено з гарантом освітньої (професійної/наукової) програми (керівником проектної групи) Кібербезпека
назва освітньої програми

Гарант освітньої (професійної/наукової) програми
(керівник проектної групи) Рассомахін Сергій Геннадійович

_____ Рассомахін С.Г.
(підпис) (прізвище та ініціали)

Програму погоджено методичною комісією факультету комп'ютерних наук

Протокол від "31" серпня 2020 року № 1

Голова методичної комісії факультету комп'ютерних наук

_____ Бердніков А. Г.

Додаток до робочої програми навчальної дисципліни «Системи технічного захисту інформації».

Дію робочої програми продовжено: на 2021/2022 н. р.

Заступник декана факультету з навчальної роботи

_____ Євгенія КОЛОВАНОВА

« » серпня 2021 р.

Голова методичної комісії факультету комп'ютерних наук

_____ Анатолій БЕРДНІКОВ

« » серпня 2021 р.

Програму погоджено з гарантом освітньої програми 125 «Кібербезпека»
Гарант освітньої програми 125 «Кібербезпека»

_____ Сергій РАССОМАХІН

ВСТУП

Програма навчальної дисципліни «Системи технічного захисту інформації» складена відповідно до освітньо програми підготовки першого (бакалаврського) рівня за спеціальністю 125 «Кібербезпека», освітня програма «Кібербезпека».

.

1. Опис навчальної дисципліни

1.1. Мета навчальної дисципліни

Дисципліна має на меті є закладання термінологічного фундаменту, отримання студентами необхідних знань щодо проявлення технічних каналів витоку інформації, шляхів деструктивного впливу на інформацію та засоби її обробки, застосування заходів та засобів, спрямованих на технічний захист інформації на об'єктах інформаційної діяльності, алгоритмів розробки та реалізації заходів захисту, у тому числі і заходів захисту інформації з обмеженим доступом.

1.2. Основні завдання дисципліни:

Основними завданнями вивчення дисципліни є:
формування у студентів певних знань та вмінь з теорії та практики організації технічного захисту інформації на об'єктах інформаційної діяльності.

1.3. Кількість кредитів – 4.

1.4. Загальна кількість годин – 120.

1.5. Характеристика навчальної дисципліни	
Нормативна	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
3-й	-й
Семестр	
5-й	-й
Лекції	
32 год.	год.
Практичні, семінарські заняття	
32 год.	год.
Самостійна робота	
56 год.	год.
Індивідуальне завдання дослідження сучасної СТЗІ 4 год.	

1.6. Заплановані результати навчання:

У результаті вивчення даного курсу студент повинен:

- знати:

1. Загальну парадигму захисту інформації.
2. Можливі технічні канали витоку інформації (ТКВІ) та фізичні явища, притаманні їх прояву та існуванню на об'єкті інформаційної діяльності (ОІД).
3. Принципи дії засобів захисту інформації, їх основні характеристики та можливості.
4. Типові заходи технічного захисту інформації (ТЗІ) на об'єктах технічних засобів прийому, передачі обробки та збереження інформації (ТЗПІ).
5. Порядок розробки та реалізації заходів ТЗІ на об'єктах ТЗПІ.

6. Вимоги керівних документів щодо організації робіт по створенню комплексу ТЗІ на ОІД.
7. Типові канали витоку інформації з обмеженим доступом (ІзОД).
8. Типові алгоритми розробки заходів захисту ІзОД.
9. Основні способи та засоби захисту від видових розвідок.
10. Основні способи та засоби захисту від радіорозвідок.
11. Основи організації ТЗІ і контролю у державі.
12. Основні шляхи забезпечення охорони ОІД.

- уміти:

1. Виявляти ТКВІ на ОІД.
2. Розробляти пропозиції з ТЗІ на ОІД.

2. Тематичний план навчальної дисципліни

Розділ 1. Загрози інформації від технічних розвідок.

Тема 1. Вступ.

Зміст. Поняття, предмет, методи і принципи інформаційного права. Джерела інформаційного права. Інформаційне право як наука і як навчальна дисципліна. Інформаційні правовідносини.

Тема 2. Види загроз інформації та їх джерела.

Зміст: від Кого Захищати Інформацію та їх загрози щодо інформації. Той, хто бажає несанкціоновано отримати інформацію – правопорушник – має можливості правові , технічні, соціальні . Юридичні можливості захисту. Соціальні можливості захисту . Технічні можливості захисту. Системність та системи технічного захисту інформації. Розвідки та їх можливості. Види розвідок та їх методи отримання інформації: агентурна, технічна. Розвідки та методи, які вони застосовують: дипломатія, хімічні речовини, НЛП, гіпноз, техніка: системи, прилади та пристрої. Комплексна протидія розвідкам.

Тема 3. Зони розташування ОІД та режими забезпечення захисту інформації.

Зміст. Варіанти розташування інформаційного об’єкту. Зони щодо захисту інформації. Пропускний режим. Внутрішньо-об’єктовий режим. Носії інформації: основні та допоміжні згідно Загальної парадигми захисту інформації. Стаціонарне розташування основних носіїв інформації. Мобільні засоби розташування носіїв інформації. Природне середовище (середовища впливу) що оточує носії інформації.

Тема 4. Контраст та демаскуючі ознаки.

Зміст: Контраст. Демаскуючі ознаки предметів (статика). Демаскуючи ознаки процесів (динаміка). Практика боротьби з інформаційною компонентою в сигналі на границі контрольованої зони. Боротьба з демаскуючими ознаками предметів. Боротьба з демаскуючими ознаками процесів.

Тема 5. Агентурна розвідка (АР) та її методи.

Зміст: Призначення АР. Методи АР. Засоби АР. Протидія АР. Нейролінгвістичне програмування, Сенсоріка НЛП. Практика НЛП.

Тема 6. Технічна розвідка

Зміст: Адаптування людських сенсорних здібностей до параметрів факторів середовища впливу. Демаскуючи ознаки – Контраст – Технічні канали витоку Інформації . Загальна характеристика Каналів витоку інформації. Речовинні КВІ. Польові КВІ.

Розділ 2. Боротьба з каналами витоку інформації.

Тема 7. Звук як шлях поширення інформації.

Зміст: Джерела звуку, динамічний та частотний діапазони. Звук як речовинні акустичні хвилі – поширення відбиття, поглинання. Фізичні середовища поширення звуку.

Акустичні лінії зв'язку. Поширення звуку. Сейсмоакустична локація заглиблених об'єктів. Методи та засоби боротьби з акустичним каналом витоку інформації.

Тема 8. Оптичне випромінювання – середовище поширення інформації.

Зміст: Джерела випромінювання, динамічний та частотний діапазони. Оптичне випромінювання як поле – поширення відбиття, поглинання: випромінювання енергії нагрітими предметами; когерентне випромінювання – лазери, мазери та ін.; поглинання енергії випромінювання. Природні та техногенні середовища поширення оптичного випромінювання. Прилади для спостереження та фіксації енергії оптичного випромінювання.

Тема 9. Виток інформації з оптичних ліній зв'язку.

Зміст: Поширення випромінювання в ВОЛЗ. Протидія перехопленню інформації з ВОЛЗ. Протидія витоку інформації зі службових приміщень. Функціональна схема зняття інформації оптичним шляхом. Функціональні елементи лазерного мікрофону. Протидія витоку інформації з оптичних ліній зв'язку.

Тема 10. Електричне поле - канал витоку інформації.

Зміст: Електричне поле та його вплив на носії електричних зарядів (провідники, напівпровідники, діелектрики, плазма). Електричні поля техногенного середовища впливу на носії інформації. Вплив електричного поля на комп'ютерні системи та лінії зв'язку.

Заземлення, як метод боротьби з несанкціонованим обмеженням доступу до інформації. Структура силових ліній електричного поля біля різноманітних предметів техногенного середовища впливу. Іонна електроскопія. Заземлення.

Тема 11. Системи заземлення ІКС.

Зміст: Теорія застосування заземлення. Три види заземлення: захисне; робоче заземлення та заземлення системи блискавкозахисту. Вплив видів заземлення на роботу елементів інформаційно-комунікаційних систем. Захисне заземлення і занулення. Функціональні елементи заземлення. Розрахунок елементів захисного заземлення. Вивчення елементів заземлення на реальному об'єкті інформаційної діяльності.

Тема 12. Прикладні елементи теорії поля.

Зміст: Теорія поля. Рівняння Максвелла. Електромагнітне поле (ЕМП). Поширення інформації електромагнітним полем. Джерела випромінювання електромагнітного поля. Енергії та частотні діапазони природних джерел електромагнітного поля. Поширення інформації електромагнітним полем різних діапазонів частот.

Тема 13. Загрози інформації що поширюється ЕМП.

Зміст: Лінії зв'язку з застосуванням ЕМП та загрози інформації. Методи перехоплення інформації в лініях радіозв'язку. Частотні спектри сигналів. Види модуляції та їх завадостійкість. Вивчення методів протидії НСД с застосуванням ЕМП. Радіолокація. Радіомікрофон.

Тема 14. Загрози інформації для систем мобільному зв'язку.

Зміст: Системи мобільного зв'язку. Організація стільникового зв'язку та принципи роботи. Методи перехоплення інформації, що передається мобільними системами зв'язку. Захист інформації , що передається мобільними системами зв'язку. Вивчення методів протидії НСД при користуванні мобільним зв'язком. Пасивні методи протидії НСД. Активні методи протидії НСД. Боротьба з радіоподавленням цифрового каналу зв'язку.

Тема 15. Ядерно-фізичні методи виявлення вибухових пристроїв, зброї та радіоактивних речовин.

Зміст: Радіоактивність. Причини і властивості. Апаратура та методи вимірювання радіоактивності для боротьби з ядерним тероризмом. Рентгеноінтраскопія. Радіаційне обстеження приміщень об'єкта інформаційної діяльності. Характеристики радіаційних матеріалів. Період напіврозпаду. Наслідки впливу радіації на роботу комп'ютерної

елементної бази та персонал об’єкта інформаційної діяльності. Методи виявлення радіоактивних джерел.

Тема 16. Канали витоку інформації нетрадиційної природи.

Зміст: 22-й параграф книги: «Ландау, Л. Д., Лифшиц, Е. М. Теория поля. — Издание 4-е, исправленное и дополненное. — М.: Физматгиз, 1962. — 424 с. — («Теоретическая физика», том II). Преміальна робота Грігорія Перельмана щодо реальної структури поля. Роботи Ю.Козирева та інших дослідників щодо фіксації полів невиявленої природи. Експерименти В.І.Коробейникова щодо фіксації діаграми випромінювання HZ – антен. Вивчення робот: 1. Serge Kernbach, Vitaliy Zamsha, Yuri Kravchenko, “Long and Super-Long Range device-device and operator-device Interactions”, International Journal of Unconventional Science, 1(1), 24-42, 2013 (Engl.). 2. Victor Shkatov & Vitaliy Zamsha - Torsion Field and Interstellar Communication - Издание 1-е, EasyPrint, China, 2015, 32 с. Методи та апаратура виявлення каналів витоку інформації нетрадиційної природи.

Тема 17. Перспективні методи та засоби захисту інформації.

Зміст: Сучасні методи захисту інформації в ІКС. Засоби захисту інформації в ІКС. Нові сучасні прилади та пристрої захисту інформації. Методи виявлення джерел радіовипромінювання та обстеження приміщень. Сучасні методи виявлення джерел радіовипромінювання. Експериментальне дослідження випромінювання при роботі персонального комп’ютера. Практична робота з сучасними приладами типу «Сова», «RD-16M», «RD-17» та ін.

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	С. р.		л	п	лаб.	Інд.	С. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Загрози інформації від технічних розвідок.												
Тема 1. Поняття і класифікація інформації Поняття, предмет, методи і принципи інформаційного права.	8	2	2			4						
Тема 2. Види загроз інформації та їх джерела. Розвідки та їх можливості.	8	2	2			4						
Тема 3. Зони розташування ОІД та режими забезпечення захисту інформації. Розташування інформаційного об’єкту. Зони та режими	8	2	2			4						

Тема 4. Забезпечення процесу створення СТЗІ. Контраст та демаскуючі ознаки. Практика приховування інформаційної компоненти від конкурента.	8	**2**	2			4						
Тема 5. Агентурна розвідка (АР) та її методи. Нейролінгвістичне програмування	8	**2**	2			4						
Тема 6. Технічна розвідка. Загальна характеристика каналів витоку інформації.	10	**2**	2			6						
Разом за 1-й розділ	50	**12**	**12**			**26**						
Розділ 2. Боротьба з каналами витоку інформації.												
Тема 7. Звук як шлях поширення інформації. Акустичні лінії зв'язку.	10	2	2			6						
Тема 8. Оптичне випромінювання – середовище поширення інформації.	6	2	2			4						
Тема 9. Виток інформації з оптичних ліній зв'язку. Протидія витоку інформації зі службових приміщень	6	1	2			2						
Тема 10. Електричне поле - канал витоку інформації. Електричне поле як багатофакторна загроза інформації.	6	2	2			2						
Тема 11. Системи заземлення ІКС. Захисне заземлення і занулення.	6	**2**	2			**2**						
Тема 12. Прикладні елементи теорії поля. Поширення інформації електромагнітним полем.	6	**2**	2			**2**						
Тема 13. Загрози інформації що	8	**2**	2			4						

поширюється ЕМП. Вивчення методів протидії НСД с застосуванням ЕМП.												
Тема 14. Загрози інформації для систем мобільному зв'язку. Вивчення методів протидії НСД при користуванні мобільним зв'язком	6	**2**	2			**2**						
Тема 15. Ядерно-фізичні методи виявлення вибухових пристроїв, зброї та радіоактивних речовин. Радіаційне обстеження приміщень об'єкта інформаційної діяльності.	6	**1**	1			**2**						
Тема 16. Канали витоку інформації нетрадиційної природи. Практичне вивчення каналів витоку інформації нетрадиційної природи.	6	**2**	1			**2**						
Тема 17. Перспективні методи та засоби захисту інформації. Методи виявлення джерел радіовипромінювання та обстеження приміщень.	6	**2**	2			**2**						
Разом за 2-й розділ	70	**20**	**20**			**30**						
Усього годин в 5 семестрі	**120**	**32**	**32**			**56**						

4. Теми семінарських (практичних, лабораторних) занять

№ з/п	Назва теми	Кількість годин
1	Розташування інформаційного об'єкту.	**2**
2	Зони та режими.	**2**
3	Практика приховування інформаційної компоненти від конкурента.	**2**
4	Нейролінгвістичне програмування	**2**
5	Загальна характеристика каналів витоку інформації.	**2**
6	Акустичні лінії зв'язку.	**2**
7	Виток інформації з оптичних ліній зв'язку.	**2**
8	Протидія витоку інформації зі службових приміщень	**2**

9	Електричне поле як багатофакторна загроза інформації.	**2**
10	Захисне заземлення і занулення.	**2**
11	Поширення інформації електромагнітним полем.	**2**
12	Вивчення методів протидії НСД с застосуванням ЕМП.	**2**
13	Вивчення методів протидії НСД при користуванні мобільним зв'язком	**2**
14	Радіаційне обстеження приміщень об'єкта інформаційної діяльності.	**2**
15	Практичне вивчення каналів витоку інформації нетрадиційної природи.	**2**
16	Методи виявлення джерел радіовипромінювання та обстеження приміщень.	**2**
		32

5. Самостійна робота

№ з/п	№ теми	Кількість годин	Форма контролю
1	1	**4**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
2	2	**4**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
3	3	**4**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
4	4	**4**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
5	5	**4**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
6	6	**6**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
7	7	**4**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
8	8	**4**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
9	9	**2**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
10	10	**2**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
11	11	**2**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
12	12	**2**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
13	13	**2**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
14	14	**2**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
15	15	**2**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
16	16	**2**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.
17	17	**2**	Тестування якості підготовки студента з допомогою тестів в системі Moodle на сервері Центру електронного навчання.

18		**4**	Індивідуальне завдання дослідження сучасної СТЗІ

6. Індивідуальні завдання

Кожен студент в процесі підготовки до одного з практичних занять отримає за два тижні індивідуальне завдання дослідження сучасної СТЗІ.

Доповідь студента оцінює група на практичному занятті.

Розгляд двох однакових СТЗІ забороняється.

Час доповіді та оцінювання обмежені розкладом проведення практичного заняття.

7. Методи навчання

Як правило лекційні та практичні заняття проводяться аудиторне. В умовах дії карантину заняття проводяться відповідно до Наказу ректора Харківського національного університету імені В.Н. Каразіна (аудиторне або дистанційно за допомогою платформ Google Meet або Zoom).

8. Методи контролю

Поточний контроль роботи студентів при вивченні дисципліни здійснюється на лекціях у вигляді летючок (поточне тестування), практичних заняттях (постійно) шляхом проведення контрольного опитування а також з застосуванням тест-системи Moodle на сервері Центру ЕН. Підсумковий контроль здійснюється при проведенні семестрового іспиту.

Оцінювання знань на іспиті має ваговій рівень 40 (сорок) балів за три правильних відповіді на три питання в білеті. Кожен білет містить три питання згідно тематики дисципліни. Відповідь на теоретичне (перше) питання важить 10 балів. Відповіді на інші два питання мають вагу 15 балів за кожну правильну відповідь.

Оцінювання знань на іспиті по системі Moodle має ваговій рівень 40 (сорок) балів. При цьому студент в тестовому режимі відповідає на 40 запитань протягом 40 хвилин, отримуючи 1 бал за кожну правильну відповідь.

9. Схема нарахування балів

Бали за поточний контроль знань по розділах 1 та 2 протягом семестру (по темах), що нараховує тест-система Moodle на сервері Центру ЕН																	Контрольна робота.	Разом сума балів у семестрі	Іспит	Загальна сума балів
Т 1	Т 2	Т 3	Т 4	Т 5	Т 6	Т 7	Т 8	Т 9	Т 10	Т 11	Т 12	Т 13	Т 14	Т 15	Т 16	Т 17				
1	1	1	2	2	2	4	4	4	4	4	4	4	4	4	3	2	10	60	40	100

Т1, Т2, Т3, Т4 ... Т17 – теми занять.

Рівень знань, продемонстрований студентами, оцінюється таким чином:

- за темою 1(Т1) – 1 бал: 1 заняття, 1 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 2 –1 бал: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 3 – 1 бал: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 4 – 2 бали: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 5 – 2 бали: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 6 – 2 бали: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 7 – 4 бали: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 8 – 4 бали: 1 заняття, 1 тест-опитування в системі Moodle на сервері Центру ЕН;

- за темою 9 – 4 бали: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 10 – 4 бали: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 11 – 4 бали: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 12 – 4 бали: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 13 – 4 бали: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 14 – 4 бали: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 15 – 4 бали: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 16 – 3 бали: 2 заняття, 2 тест-опитування в системі Moodle на сервері Центру ЕН;
- за темою 17 – 2 бали: 2 заняття, 2 тест-опитування системі Moodle на сервері Центру ЕН;
- за контрольну роботу (Т1 – Т17) – 10 балів.

При розробці тестів тест-опитувань в системі Moodle на сервері Центру ЕН використовувалися наступні критерії для кожної групи питань по кожній з 17-ти тем (п.8):

Визначення	Кількість балів по кожній з 30-ти навчальних тем, в процентному відношенні від максимального значення, вказаного в таблиці **п.8.**
Дані повні відповіді на кожне питання, показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки	100%
У відповідях на поставлені питання показано знання навчального матеріалу, розуміння суті поставлених питань за наявності незначних помилок зроблені достатньо повні і правильні висновки	75%
У відповідях на поставлені питання показано достатньо знання навчального матеріалу при наявності суттєвих помилок, зроблені висновки	50%
У відповідях показано розуміння суті поставлених питань за наявності принципових помилок при рішенні практичних завдань, відсутні висновки	25%
У відповідях на показано слабкі знання навчального матеріалу при наявності принципових помилок при рішенні практичних завдань, відсутні висновки	0%

10. Критерії оцінювання

знань студентів на тест-опитування в системі Moodle на сервері Центру ЕН

Критерії оцінювання знань студентів за виконання контрольної роботи

Визначення	Кількість балів
Дані повні відповіді на кожне практичне питання показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки	10

У відповідях на поставлені практичні питання показано знання навчального матеріалу, розуміння суті поставлених питань за наявності незначних помилок зроблені достатньо повні і правильні висновки	7-9
У відповідях на поставлені практичні питання показано достатньо знання навчального матеріалу при наявності суттєвих помилок, зроблені висновки	5-6
У відповідях показано розуміння суті поставлених питань за наявності принципових помилок при рішенні практичних завдань, відсутні висновки	4
У відповідях на показано слабкі знання навчального матеріалу при наявності принципових помилок при рішенні практичних завдань, відсутні висновки	2

Критерії оцінювання екзаменаційних робіт студентів

Визначення	Кількість балів
При відповіді на екзаменаційний білет питання освітлені повністю, завдання вирішене правильно, зроблені висновки	40
При відповіді на екзаменаційний білет питання достатньо освітлені, завдання вирішене правильно з незначними помилками, зроблені висновки	35-39
При відповіді на екзаменаційний білет питання освітлені з помилками, завдання вирішене правильно з незначними помилками. Зроблені неповні висновки	25-34
При відповіді на екзаменаційний білет питання освітлені з суттєвими помилками, завдання вирішене з помилками. Зроблені неповні висновки	15-24
При відповіді на екзаменаційний білет питання освітлені з суттєвими помилками, завдання вирішене частково або не повністю. Висновки неповні або відсутні	1-14

11. Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка
	для чотирирівневої шкали оцінювання (іспит)
90 – 100	відмінно
70-89	добре
50-69	задовільно
1-49	незадовільно

12. Рекомендована література

12. Рекомендована література

Базова

1. Методи та засоби технічного захисту інформації. Опорний конспект лекцій [Електронний ресурс] : навч. посіб. для здобувачів ступеня бакалавра за освітньою програмою «Системи технічного захисту інформації» спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: В. М. Луценко, Д. О. Прогонов. – Електронні текстові дані (1 файл: 37,65 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 289 с.

2. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

3. Пархуць Л.Т. Методи і засоби захисту інформації. Конспект лекцій. Частина 1. «Захист інформації від витоку по технічних каналах». НУ ЛП, — Львів: 2008. — 67с. Частина 2. «Методи і засоби пошуку електронних пристроїв перехоплення інформації». НУ ЛП, — Львів: 2009. — 84с.

4. В.А.Хорошко, А.А.Чекатков. Методи та засоби захисту інформації.: Київ. - Юніор, 2003. – 504 с.

5. Єсін В. І. Безпека інформаційних систем та технологій / В. І. Єсін, А. А. Кузнєцов, Л. С. Сорока. - Харків: ТОВ «ЕДЕНА», 2010. - 656 с.

6. «Актуальні проблеми кібербезпеки та захисту інформації»: тези доповідей семінару кафедри Систем інформаційного та кібернетичного захисту від 07 травня 2019 року – Київ: - ДУТ, 2019 – 31с.

7. Лєнков С.В., Перегудов Д.А., Хорошко В.А. Методи та засоби захисту інформації. Т2 - Інформаційна безпека. – Київ: «Арій», 2008, – 344 с

Допоміжна

1. ДСТУ 3396.0-96 Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення.

2. ДСТУ 3396.1-96 Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

3. ДСТУ 3396.2-97 Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення

4. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

5. НД ТЗІ 1.1-005-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення»

6. НД ТЗІ 3.1-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи»

7. НД ТЗІ 3.3-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації»

8. НД ТЗІ 2.1-002-07 «Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення».

9. ТПКО-95 Тимчасове положення з категоріювання ОІД.

10. ДБН А.2.2-2-96 ДЕРЖАВНІ БУДІВЕЛЬНІ НОРМИ УКРАЇНИ. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва.

11. Положення про державний контроль за станом технічного захисту інформації від 16.05.2007 №87.13.

14. Bluetooth [Електронний ресурс] // Bluetooth – Режим доступу: https://www.bluetooth.com/about-us (дата звернення: 01.11. 2018р).

15. Блатова Т. А. Управління інноваційним розвитком галузі інформаційно-телекомунікаційних технологій // Актуальні проблеми інфотелекоммунікацій в науці та освіті: збірник наукових статей в 2 томах. - 2015. – с. 709-713

Додаток до робочої програми навчальної дисципліни «Системи технічного захисту інформації».

Дію робочої програми продовжено: на 2021/2022 н. р.

Заступник декана факультету з навчальної роботи

_____ Євгенія КОЛОВАНОВА

« » серпня 2021 р.

Голова методичної комісії факультету комп'ютерних наук

_____ Анатолій БЕРДНІКОВ

« » серпня 2021 р.

Програму погоджено з гарантом освітньої програми 125 «Кібербезпека»
Гарант освітньої програми 125 «Кібербезпека»

_____ Сергій РАССОМАХІН