ЗАТВЕРДЖЕНО
Вченою радою факультету
інформаційно-комп'ютерних технологій
31 серпня 2023 р., протокол № 5
Голова Вченої ради
Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 30 «КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека та захист інформаційя»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної інженерії та кібербезпеки
28 серпня 2023 р., протокол № 7
Завідувач кафедри
Андрій ЄФІМЕНКО
Гарант освітньо-
професійної програми
Андрій ЄФІМЕНКО

Розробник: кандидат технічних наук, доцент кафедри комп'ютерної інженерії та кібербезпеки Пірог Олександр Вікторович

Житомир
2026-2027 н.р.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітній ступінь	Характеристика навчальної дисципліни
		денна форма навчання
Кількість кредитів 4	Галузь знань 12 «Інформаційні технології»	за вибором
Модулів – 1	Спеціальність 125 «Кібербезпека»	Рік підготовки:
Змістових модулів – 2		4
		Семестр
Загальна кількість годин - 120		2
		Лекції
Тижневих годин для денної форми навчання: аудиторних – 4 самостійної роботи – 6	Освітній ступінь «бакалавр»	24 год.
		Практичні
		__ год.
		Лабораторні
		24 год.
		Самостійна робота
		72 год.
		Вид контролю: залік

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 40 % аудиторних занять, 60 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Мета навчальної дисципліни полягає у формуванні у майбутніх спеціалістів знань, умінь та компетенцій в сфері комплексного захисту інформації (КСЗІ) в інформаційно-телекомунікаційних системах (ІТС) від основних загроз здійснення несанкціонованого доступу (НСД) до інформації та руйнування інформації.

Завданнями вивчення навчальної дисципліни є формування теоретичних знань та практичних умінь у сфері КСЗІ, в тому числі;

– знати цілі, завдання та принципи створення КСЗІ;

– знати основні терміни та визначення в галузі КСЗІ;

– знати законодавство України в області захисту інформації, положення правових норм щодо створення КСЗІ та комплексів ТЗІ, КЗІ;

– знати основні способи здійснення НСД до інформації в ІТС;

– знати основні загрози та типи атак на в ІТС;

– знати основні канали витоку інформації в ІТС;

– знати методи, засоби та заходи захисту інформації в ІТС від НСД;

– знати основні методи і засоби руйнування інформації в ІТС;

– знати методи, засоби та заходи захисту інформації в ІТС від руйнування;

– вміти аналізувати, виявляти та оцінювати можливі загрози інформації в ІТС;

– вміти розробляти моделі загроз та моделі порушника в ІТС;

– вміти розробляти, впроваджувати та забезпечувати функціонування КСЗІ;

– вміти забезпечувати захист інформації в ІТС;

– вміти вирішувати задачі протидії НСД до інформації в ІТС;

– вміти проводити атестацію режимних територій (зон), приміщень.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації»:

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області та розуміння професії.

КФ1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

КФ2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових,

організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

КФ10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

КФ12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 125 «Кібербезпека та захист інформації»:

РН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

РН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

РН33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

РН35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.

РН39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

РН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

3. Програма навчальної дисципліни

Змістовий модуль 1. Основні поняття та положення щодо створення КСЗІ в Україні.

Тема 1. Концепція інформаційної безпеки.

Основні положення системи захисту інформації (СЗІ). Вимоги безпеки СЗІ. Умови безпеки СЗІ. Види забезпечення безпеки СЗІ. Концептуальна модель інформаційної безпеки, її основні компоненти. Інформаційна безпека. Загрози інформації та їх прояви. Класифікація загроз. Дії, які призводять до неправомірного оволодіння інформацією з обмеженим доступом. Технічний

канал витоку інформації.

Тема 2. Комплексна система захисту інформації: цілі, завдання, принципи створення.

Комплексна система захисту інформації (КСЗІ). Цілі та завдання КСЗІ. Склад КСЗІ. Об'єкти захисту в інформаційно-телекомунікаційних системах (ІТС). Суб'єкти інформаційних відносин в ІТС. Принципи створення КСЗІ. Основні вимоги до КСЗІ.

Тема 3. Основні терміни та визначення.

Інформація. Документ. Електронний документ. Електронний підпис. Ліцензія. Ліцензування. Інформаційна безпека. Безпека інформації. Об'єкт інформаційної діяльності (ОІД). Державна таємниця (секретна інформація). Гриф секретності. Засекречування матеріальних носіїв інформації. Категорія режиму секретності. Матеріальні носії секретної інформації. Охорона державної таємниці. Ступінь секретності. Інформаційна (автоматизована) система. Інформаційно-телекомунікаційна система (ІТС). Телекомунікаційна система. Обробка, блокування, виток, знищення, захист інформації. Доступ до інформації. Криптографічний захист інформації (КЗІ). Несанкціоновані дії. Несанкціонований доступ (НСД) до інформації. Порушення цілісності інформації в системі. Порядок доступу до інформації. Технічний захист інформації (ТЗІ). Автоматизовані системи (АС) різних класів. Обчислювальна система (ОС). Комп'ютерна система. Політика безпеки інформації. Загроза. Атака. Комплекс засобів захисту. Конфіденційність, цілісність інформації. Система ТЗІ. Технічний канал витоку інформації. Побічне електромагнітне випромінювання і наведення. Контрольована зона.

Тема 4. Законодавство України в області захисту інформації.

Система нормативно-правових документів в Україні, що регламентують питання захисту інформації. Структура законодавства України в області захисту інформації. Конфіденційна інформація. Основні параметри комерційної таємниці. Правові норми забезпечення безпеки і захисту інформації на конкретному підприємстві.

Тема 5. Основні положення правових норм щодо створення КСЗІ та комплексів ТЗІ і КЗІ.

Основні напрями державної інформаційної політики. Суб'єкти і об'єкт інформаційних відносин. Сфери, у яких інформація може бути віднесена до державної таємниці. Основні організаційно-правові заходи щодо охорони державної таємниці. Загрози національним інтересам і національній безпеці України в інформаційній сфері. Основні напрями державної політики з питань національної безпеки в інформаційній сфері. Об'єкти та суб'єкти захисту в ІТС. Ліцензування послуг в галузі ТЗІ, КЗІ. Правопорушення та злочини в галузі захисту інформації. Положення про ТЗІ і КЗІ в Україні. Основні функції організаційних структур системи ТЗІ. Основні напрями державної політики у

сфері ТЗІ. Нормативні документи з технічного захисту інформації: ДСТУ, ДБН, тимчасові регламенти, нормативні документи.

Змістовий модуль 2. Методи, засоби та заходи захисту інформації в ІТС від НСД, витоку та руйнування.

Тема 6. Несанкціонований доступ до інформації і способи його здійснення.

Способи здійснення НСД. Модель способів НСД до джерел інформації. Основні задачі НСД. Класифікація загроз безпеки ІТС. Причини випадкових дій. Умисні загрози. Інсайдер. Основні канали НСД. Перехоплення паролів. Маскарад. Незаконне використання привілеїв. Шкідливі програми. Градації доступу до інформації. Напрями реалізації порушником інформаційних загроз в ІТС. Методи реалізації загроз НСД.

Тема 7. Мережеві атаки та модель порушника.

Аналіз загроз корпоративних мереж. Типи мережевих атак: атаки доступу, модифікації, відмова в обслуговуванні, Комбіновані атаки: підміна довіреного суб'єкта, посередництво (атака Man-inthe-Middl – «людина-в-середині»), експлойти, парольні атаки (спуфинг, сніфинг, простий перебір (Brute Force Attack)), вгадування ключа, атаки на рівні застосувань, аналіз мережевого трафіку, мережева розвідка, зловживання довірою, псевдоантивіруси, фішинг, фарминг, застосування ботнетів, розсилка спаму, анонімний доступ в мережу, крадіжка конфіденційних даних. Основні причини атак на IP-мережі. Загрози при безпровідному доступі до локальної мережі: виявлення WLAN, підслуховування, фальшиві точки доступу в мережу, відмова в обслуговуванні, атаки типу «людина-в-середині», анонімний доступ в Інтернет. Тенденції розвитку ІТ-загроз. Сценарії розвитку ІТ-загроз на найближчий час. Модель порушника.

Тема 8. Методи, засоби та заходи захисту інформації в ІТС від НСД.

Основні принципи забезпечення захисту інформації від НСД. Планування захисту і керування системою захисту. Керування системою доступу. Безперервний захист. Атрибути доступу. Концепція матриці доступу. Довірче і адміністративне керування доступом. Забезпечення персональної відповідальності. Послуги безпеки. Політика безпеки. Основні принципи реалізації програмно-технічних засобів захисту інформації в ІТС від НСД: Концепція диспетчера доступу. Ядро захисту.

Тема 9. Технічні канали витоку відео та акустичної інформації.

Спостереження за об'єктом. Класифікація способів прихованого відеоспостереження і зйомки. Характеристика технічних каналів витоку акустичної інформації. Причини створення акустичних каналів витоку інформації. Канали витоку акустичної інформації з об’єктів інформаційної діяльності (ОІД). Класифікація технічних каналів витоку акустичної інформації: повітряні, вібраційні, електроакустичні, оптико-електронні.

Тема 10. Технічні канали витоку інформації, що обробляється технічними засобами обробки інформації.

Технічні засоби обробки інформації (ТЗОІ). Допоміжні технічні засоби і системи (ДТЗС). Контрольована зона (КЗ). Межа КЗ. Виділені приміщення (ВП). Об'єкти засобів обчислювальної техники (ЗОТ). Об’єкт інформатизації, як об’єкт розвідки. Технічний канал витоку інформації (ТКВІ). Технічні засоби розвідки (ТЗР). Спеціальні технічні засоби (СТЗ). Класифікація ТКВІ в ІТС. Електромагнітні канали витоку інформації. Причини виникнення електромагнітних каналах витоку інформації. Режими оброблення інформації в засобах обчислювальної техніки (ЗОТ), в яких виникає побічне електромагнітне випромінювання (ПЕМВ). Паразитне електромагнітне випромінювання ТЗОІ. Технічні засоби розвідки побічних електромагнітних випромінювань і наведень (ТЗР ПЕМВН). Електричні канали витоку інформації (ЕКВІ). Небезпечна зона. Виток інформації за рахунок наведень. Спеціально створювані технічні канали витоку інформації. Виток інформації створений шляхом високочастотного опромінення. Закладні пристрої. Класифікація апаратних закладних пристроїв: перехоплення зображень монітора, перехоплення інформації з клавіатури, комплексне перехоплення інформації.

Тема 11. Методи і засоби руйнування інформації.

Умисна силова електромагнітна дія. Причини умисного руйнування інформації. Методи руйнування інформації. Завади. Навмисні силові впливи (НСВ): мережами живлення, дротяними лініями зв'язку, безпровідний. Шкідливе програмне забезпечення (ШПЗ). Програмне заглушення обчислювальних систем (ПрЗ ОС). Методи заглушення ОС процедурними і декларативними ПрЗ. Методи впливу ПрЗ на програмне і апаратне забезпечення ОС. Метод впливу ПрЗ на операторів ОС. Закладні пристрої (апаратні і програмні).

Тема 12. Захист інформації в ІТС від витоку та руйнування.

Загальні рекомендації з ТЗІ з обмеженим доступом від витоку каналами ПЕМВН. Організаційні заходи. Підготовчі технічні заходи: блокування каналів можливого витоку інформації з обмеженим доступом (ІзОД). Технічні заходи. Засоби технічного захисту. Порядок контролю за станом ТЗІ.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	практичні	самостійна робота	усього	лекції	практичні	самостійна робота
Змістовий модуль 1. Основні поняття та положення щодо створення КСЗІ в Україні								
Тема 1. Концепція інформаційної безпеки	8	2		6				
Тема 2. Комплексна система захисту інформації: цілі, завдання, принципи створення	8	2		6				
Тема 3. Основні терміни та визначення	12	2	4	6				
Тема 4. Законодавство України в області захисту інформації	8	2		6				
Тема 5. Основні положення правових норм щодо створення КСЗІ та комплексів ТЗІ і КЗІ	8	2		6				
Разом за змістовий модуль 1	44	10	4	30				
Змістовий модуль 2. Методи, засоби та заходи захисту інформації в ІТС від НСД, витоку та руйнування								
Тема 6. Несанкціонований доступ до інформації і способи його здійснення	12	2	4	6				
Тема 7. Мережеві атаки та модель порушника	12	2	4	6				
Тема 8. Методи, засоби та заходи захисту інформації в ІТС від НСД	12	2	4	6				
Тема 9. Технічні канали витоку відео та акустичної інформації	10	2	2	6				
Тема 10. Технічні канали витоку інформації, що обробляється технічними засобами обробки інформації	10	2	2	6				
Тема 11. Методи і засоби руйнування інформації	10	2	2	6				
Тема 12. Захист інформації в ІТС від витоку та руйнування	10	2	2	6				
Разом за змістовий модуль 2	76	14	20	42				
ВСЬОГО	120	24	24	72				

5. Теми практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	СЗІ. Терміни, при створенні КСЗІ. Вибір АС, що буде досліджуватися.	2	
2	Виявлення основних активів, що потребують захисту. Розробка завдань захисту інформації в АС.	2	
3	Розробка опису компонентів АС та технологій обробки інформації.	2	
4	Розробка класифікації інформації, що обробляється в АС, об’єктів, де вона циркулює, та доступу до неї персоналу.	2	
5	Виявлення можливих порушників, їх типізація та розробка типових моделей порушників.	2	
6	Розробка моделі загроз в АС.	2	
7	Аналіз та оцінка ризиків. Оцінювання величини можливих збитків, пов'язаних з реалізацією загроз. Вибір варіанту побудови КСЗІ. Оцінювання витрат на КСЗІ. Вибір основних рішень забезпечення безпеки інформації на 3 рівнях: правовому, організаційному, технічному. Розробка політики безпеки інформації в АС.	6	
8	Підготовка звітних документів по результатах аналізу моделі загроз та вибору політики безпеки. Розробка плану захисту інформації в АС. Розробка акта категоріювання АС. Підготовка акту обстеження на ОІД.	4	
12	Підсумкові заняття: захист лабораторних робіт	2	
РАЗОМ		24	

6. Завдання для самостійної роботи

Тема 1. Стандарти управління інформаційною безпекою (СУІБ).

Тема 2. Електронний документообіг.

Тема 3. Методика формування нормативних, розпорядчих та методичних документів в процесі впровадження та функціонування СУІБ.

Тема 4. Організаційна структура служби інформаційної безпеки.

Тема 5. Методи оброблення ризиків.

Тема 6. Формування ситуаційного плану.

Тема 7. Сімейство міжнародних стандартів ISO.

Тема 8. Радіозакладні пристрої та методи їх маскування.

Тема 9. Стійкість парольного захисту.

Тема 10. Стійкість точок доступу бездротової мережі Wi-Fi.

Тема 12. Аутентифікація користувачів на основі токенів безпеки.

7. Індивідуальні завдання

(не передбачені навчальним планом)

8. Методи навчання

Навчання в аудиторіях відбувається в формі лекційних та лабораторних занять. Для полегшення засвоєння матеріалу використовуються технічні засоби.

9. Методи контролю

Навчальні досягнення студентів з дисципліни оцінюються за рейтинговою системою, в основу якої покладено принцип пооопераційної звітності, накопичувальної системи оцінювання рівня знань, умінь та навичок.

Контроль складається з поточного контролю виконання студентами самостійної роботи, контролю виконання лабораторних робіт та підсумкового контролю, в тому числі у вигляді комп'ютерних тестів, захисту лабораторних робіт у формі співбесіди. Поточний контроль здійснюється під час проведення лабораторних робіт для перевірки рівня підготовки студента до виконання конкретної роботи. Форма проведення поточного контролю: усне індивідуальне опитування. Підсумковий контроль знань студентів здійснюється після завершення вивчення навчального матеріалу у вигляді комп'ютерних тестів. Методи самоконтролю: уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за лабораторну роботу залежить від дотримання таких вимог:

- своєчасності виконання завдань;
- повноти обсягу їх виконання;
- якості виконання завдань;
- самостійності виконання;
- творчого підходу у виконанні завдань;
- ініціативності у навчальній діяльності;
- глибини розуміння теми роботи;
- якості відповідей на поставлені питання підчас захисту роботи.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до таблиці розподілу балів дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблиці шкала оцінювання.

10. Розподіл балів

Поточне тестування та самостійна робота									Сума
Л1	Л2	Л3	Л4	Л5	Л6	Л7	Л8	Тест	100
7	7	7	7	7	7	7	7	44	

Шкала оцінювання

За шкалою	Екзамен	Залік	Бали
A	Відмінно	Зараховано	90-100
B	Добре	Зараховано	82-89
C			74-81
D	Задовільно	Зараховано	64-73
E			60-63
FX	Незадовільно	Не зараховано	35-59
F		Не зараховано	0-34

11. Рекомендована література

Основна література

1. Бобало Ю. Я. Стратегічна безпека системи “об’єкт – інформаційна технологія” / Ю.Я.Бобало, В.Б.Дудикевич, Г.В.Микитин.– 2020.– 260с.
2. Гребенніков В. Комплексні системи захисту інформації. Проектування, впровадження, супровід / В.Гребенніков.– 2019.
3. Козюра В.Д. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В.Д.Козюра, В.О.Хорошко, М.Є.Шелест, Ю.М.Ткач, Я.Ю.Усов. – Ніжин: ТПК «Орхідея», 2019. – 144 с.
4. Хорошко В.О. Проєктування комплексних систем захисту інформації / Ю.Я.Бобало, І.М.Павлов.– Львів: Видавництво Львівської політехніки, 2020.– 320 с.
5. Яремчук Ю.Є. Комплексні системи захисту інформації / Ю.Є.Яремчук, П.В.Павловський, В.С.Катаєв, В.В.Сінюгін.– Вінниця: ВНТУ, 2017. – 120 с.
6. Brotherston L. Defensive Security Handbook: Best Practices for Securing Infrastructure / L.Brotherston.– 2017.– 274 p.

Нормативні документи

1. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. – URL: https://zakon.rada.gov.ua/laws/show/3475-15

2. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. – URL: https://zakon.rada.gov.ua/laws/show/3855-12

3. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. – URL: https://zakon.rada.gov.ua/laws/show/2155-19

4. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. – URL: https://zakon.rada.gov.ua/laws/show/851-15

5. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 № 518. – URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF

6. Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності, що підлягає ліцензуванню, у сфері надання послуг у галузі криптографічного захисту інформації (крім електронних довірчих послуг) та технічного захисту інформації : Постанова Кабінету Міністрів України від 31.10.2018 № 915. – URL: https://zakon.rada.gov.ua/laws/show/915-2018-%D0%BF

7. Про затвердження Методичних рекомендацій щодо категоризації об’єктів критичної інфраструктури : Наказ Адміністрації Держспецзв'язку від 15.01.2021 № 23. – URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-15-01-2021-23-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-kategorizaciyi-ob-yektiv-kritichnoyi-infrastrukturi

8. Про затвердження Положення про державну експертизу в сфері технічного захисту інформації : Наказ Адміністрації Держспецзв’язку від 16.05.2007 № 93. – URL: https://zakon.rada.gov.ua/laws/show/z0820-07

9. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом : Постанова Кабінету Міністрів України від 11.11.2020 № 1176. – URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennya-poryadku-prove-a1176

10. Про затвердження уніфікованої форми акта, складеного за результатами проведення планового (позапланового) заходу державного нагляду (контролю) щодо дотримання кваліфікованим надавачем електронних довірчих послуг вимог законодавства у сфері електронних довірчих послуг : Наказ Адміністрації Держспецзв'язку від 13.04.2020 № 204. – URL: https://zakon.rada.gov.ua/laws/show/z0385-20

11. Про затвердження уніфікованої форми акта, складеного за результатами проведення планового (позапланового) заходу державного нагляду (контролю) щодо дотримання ліцензіатом вимог ліцензійних умов у сфері провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім електронних довірчих послуг) та технічного захисту інформації за переліком, що визначається Кабінетом

Міністрів України : Наказ Адміністрації Держспецзв'язку 26.02.2020 № 117. – URL: https://zakon.rada.gov.ua/laws/show/z0381-20

12. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. – URL: https://zakon.rada.gov.ua/laws/show/80/94-вр

13. Про ліцензування видів господарської діяльності: Закон України від 02.03.2015 № 222-VIII. – URL: https://zakon.rada.gov.ua/laws/show/222-19

14. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V. – URL: https://zakon.rada.gov.ua/laws/show/537-16

15. Типове положення про службу захисту інформації в автоматизованій системі : НД ТЗІ 1.4-001-2000

Допоміжна література

1. Біленчук П.Д. Комп'ютерний тероризм: суперхакери, кібер-терористи, кібер-криміналісти: Монографія / П.Д.Біленчук, М.В.Гуцалюк, О.В.Кравчук, М.В.Козир. – К.: Наука і життя, 2008.

2. Блавацька Н.М. Програмне забезпечення систем захисту інформації : підручник / Н.М.Блавацька, В.Д.Козюра, В.О.Хорошко. – К.: Вид. ДУІКТ, 2011. – 330 с.

3. Бутузов В. М. Науково-практичний коментар до Кримінального кодексу України. Особлива частина. Розділ XVI. Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку / В.М.Бутузов, С.А.Кузьмін, В.П.Шеломенцев. – К., 2010. – 152 с.

4. Гарасимчук О.І. Комплексні системи санкціонованого доступу: навч. посібник / О.І.Гарасимчук, В.Б.Дудикевич, В.А.Ромака – Л. : Вид-во Львів. політехніки, 2010. - 212 с.

5. Коженевский С.Р. Термінологічний довідник з питань технічного захисту інформації / С.Р.Коженевский, Г.В.Кузнецов, В.О.Хорошко, Д.В.Чирков; за ред. проф. В.О.Хорошка. – К.: Вид. ДУІКТ, 2007. – 365 с.

6. Макнамара Д. Секреты компьютерного шпионажа: тактика и контрмеры / Д.Макнамара; пер. с англ.; под ред. С.М.Молявко. – М.: БИНОМ. Лаборатория знаний, 2004. – 536 с.

12. Інформаційні ресурси в Інтернеті

1. Законодавство України : Верховна рада України. – URL: https://zakon.rada.gov.ua/laws/

2. Державна служба спеціального зв’язку та захисту інформації. – URL: https://cip.gov.ua/

3. OWASP Threat Dragon Docs. – URL: https://threatdragon.github.io/