ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в інформаційно – телекомунікаційних системах
Освітньо-професійна програма «Комп'ютерна інженерія»
першого рівня вищої освіти
Спеціальність 123 Комп'ютерна інженерія
Галузь знань 12 Інформаційні технології

Розглянуто на засіданні кафедри Протокол №13 від 31.03.2022

м. Кропивницький – 2022

ЗМІСТ

1. Загальна інформація

Назва дисципліни	**Захист інформації в інформаційно – телекомунікаційних системах**
Рік викладання	2022-2023 навчальний рік
Викладач	Улічев Олександр Сергійович https://www.researchgate.net/profile/Oleksandr_Ulichev http://kbpz.kntu.kr.ua/ylichev-oleksandr/
Асистент	Поліщук Людмила Іванівна https://www.researchgate.net/profile/Liudmyla-Polishchuk http://kbpz.kntu.kr.ua/polishchuk-lyudmyla/
Контактний телефон	(0522)-390-449 – кафедра кібербезпеки та програмного забезпечення, робочі дні з 8^{30} до 14^{20}
E-mail:	askin79@gmail.com
Консультації	*Очні консультації* згідно розкладу консультацій Понеділок та Четвер з 14^{20} до 15^{30} *Онлайн консультації* за попередньою домовленістю в робочі дні з 8^{30} до 14^{20}

2. Анотація дисципліни

Дисципліна «Захист інформації в інформаційно – телекомунікаційних системах» розглядає та вивчає особливості організації та функціонування засобів зв'язку, методів пов'язаних з запобіганням комп'ютерній злочинності, а також застосуванню методів та засобів захисту інформації у сучасних інформаційних системах та мережах телекомунікаційного зв'язку в умовах широкого використання сучасних інформаційних технологій. Дисципліна відноситься до дисциплін професійного спрямування.

Дисципліна викладається на 2 курсі, базовими знаннями є знання отримані в ході вивчення дисциплін: «Базові методології та технології програмування», «Спец. розділи математики для інформаційної безпеки»

Дисципліна передбачає ознайомлення з основними поняттями захисту інформації: нормативна база інформаційної безпеки, програмні засоби ІБ, класифікація криптографічних алгоритмів, апаратні та програмно-апаратні засоби захисту та протидії інформаційному шпигунству. Дисципліна не передбачає жорстких вимог з точки зору використання мов програмування в ході виконання лабораторно-практичних завдань, лабораторні роботи можуть виконуватись з використанням інструментів та мов програмування на вибір студента. Частина практично-лабораторних робіт має пошуково-аналітичний характер, та передбачає звітність з використанням програмних додатків пакету MS Office/

3. Мета і завдання дисципліни

Метою викладання дисципліни «Захист інформації в інформаційно – телекомунікаційних системах» полягає у формуванні у майбутніх фахівців умінь та компетенцій для забезпечення ефективного захисту інформації, необхідних для подальшої роботи в організаціях за спеціалізацією, пов'язаною із боротьбою з комп'ютерною злочинністю, та навчити їх застосуванню методів та засобів захисту інформації у сучасних інформаційних системах та мережах телекомунікаційного зв'язку в умовах широкого використання сучасних інформаційних технологій.

Дисципліною передбачено, що в результаті студенти мають набути нижче зазначених знань та практичних навичок.

Студенти повинні знати:

- правову та організаційну основи забезпечення інформаційної безпеки у комп'ютерних системах і мережах, системах телекомунікаційного зв'язку та, зокрема, у системах та мережах;
- основні види загроз інформаційній безпеці в інформаційних системах і мережах та телекомунікаційних каналах зв'язку, технічні канали витоку інформації з них, методи виявлення та блокування цих каналів;
- основні види та можливості технічних та програмних методів та засобів захисту, зокрема, криптографічних і стеганографічних систем захисту інформації.

Студенти повинні вміти:

- планувати та організовувати свою роботу та роботу підрозділу з урахуванням вимог до захисту інформації з обмеженим доступом;
- планувати й організовувати роботи щодо створення та розвитку системи інформаційної безпеки у комп'ютерних системах та мережах;
- здійснювати ефективний вибір комп'ютерних систем захисту;
- оцінювати доцільність застосування того чи іншого криптопримітиву (схеми шифрування, хешування, будь-якого криптографічного протоколу) у складі комплексної системи захисту інформації.

Ці уміння необхідні на етапах проектування, розробки, експлуатації та аналізу роботи систем захисту для правильного розуміння принципів роботи, призначення та ефективності обраних засобів, які використовуються або плануються для використання в організації, що має справу з інформацією з обмеженим доступом.

4. Формат дисципліни

Для денної форми навчання:

Викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням мультимедійних презентацій, у поєднанні з лабораторними заняттями з застосуванням комп'ютерів.
Формат очний (Face to face)

Для заочної форми навчання:

Під час сесії формат очний (Face to face), у міжсесійний період – дистанційний (online).

5. Результати навчання

Програмні результати вивчення дисципліни:

Знати:

- правову та організаційну основи забезпечення інформаційної безпеки у комп'ютерних системах і мережах, системах телекомунікаційного зв'язку та, зокрема, у системах та мережах;
- основні види загроз інформаційній безпеці в інформаційних системах і мережах та телекомунікаційних каналах зв'язку, технічні канали витоку інформації з них, методи виявлення та блокування цих каналів;
- основні види та можливості технічних та програмних методів та засобів захисту, зокрема, криптографічних і стеганографічних систем захисту інформації.

Вміти:

- планувати та організовувати свою роботу та роботу підрозділу з урахуванням вимог до захисту інформації з обмеженим доступом;
- планувати й організовувати роботи щодо створення та розвитку системи інформаційної безпеки у комп'ютерних системах та мережах;
- здійснювати ефективний вибір комп'ютерних систем захисту;
- оцінювати доцільність застосування того чи іншого криптопримітиву (схеми шифрування, хешування, будь-якого криптографічного протоколу) у складі комплексної системи захисту інформації.

Набуття навичок комунікації:

- використовувати інформаційні технології та для ефективного спілкування на професійному та соціальному рівнях.

Набути навичок автономії і відповідальності:

- якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	Кількість годин
Рекомендації щодо семестру вивчення	4 семестр
Спеціальність	123 Комп'ютерна інженерія
Кількість кредитів / годин	3 / 90
Кількість змістових модулів	2
Нормативна / вибіркова	вибіркова
лекції	14
лабораторні роботи	14
самостійна робота	32
Вид підсумкового контролю: екзамен	30

7. Пререквізити

Бажане попереднє вивчення дисциплін: «Базові методології та технології програмування», «Спец. розділи математики для інформаційної безпеки», «Фізика», шкільний курс інформатики. Особливо важливими є знання та навички окремих розділів математики: «дискретна математика», «теорія чисел», «комбінаторика», а також окремих розділів фізики «хвилі, коливання», «електро-магнітні ефекти»

8. Технічне і програмне забезпечення /обладнання

Обов'язкове технічне забезпечення: для студентів ПК з доступом до мережі Інтернет для виконання лабораторних робіт, взаємодії з системою дистанційної освіти Moodle, online консультацій з викладачем; для викладача мультимедійний проектор та ноутбук для демонстрації лекційного матеріалу.

Рекомендоване програмне забезпечення: Word, PowerPoint, Notepad++, Браузер (Chrome), мова програмування та середовище (на вібір студента).

9. Політика дисципліни

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення. Детальніше за посиланням URL: http://www.kntu.kr.ua/doc/dobro.pdf

Відвідування занять:

Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і практичні заняття курсу. Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Політика щодо термінів здачі залікових робіт та КП, перескладання:	Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний, стажування або відрядження).
Політика щодо академічної доброчесності:	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).
Політика щодо відвідування:	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету).

Поведінка на заняттях:

Недопустимість: запізнень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення навчальних дисциплін вільного вибору; Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ; Кодексу академічної доброчесності ЦНТУ.

10. Тематика лекційних та практичних занять

Тиждень, дата, академічні години	Тема, основні питання	Форма діяльності (заняття) /формат	Матеріали	Література, інформаційні ресурси	Самостійна робота, завдання, години	Вага оцінки (кількість балів)	Термін виконання
Модуль 1 Загальні принципи захисту інформації в інформаційно-телекомунікаційних системах (4 семестр)							
Тиж. 1 (за розкладом) 2 год.	**Л1** **Правові та організаційні засади захисту інформації в інформаційних системах.**	Лекція / *Face to face*	Презентація	[1-11,23] – відповідні теми	Опрацювати матеріал лекції. Самостійно опрацювати матеріал: інф. джерела: 1-11,23. 2 год.	4	Самостійна робота до кінця 2 тижня
Тиж. 2 (за розкладом) 2 год.	***Практична робота №1. Аналіз законодавство України в сфері захисту інформації.***	Практична робота / *Face to face*	Методичні рекомендації	[1-11,23]] – відповідні теми	Оформити звіт з виконаної практичної роботи та підготувати відповіді на контрольні питання. 2 год.	4	Самостійна робота до кінця 2 тижня
Тиж. 3 (за розкладом) 2 год.	**Л2** **Програмні методи та засоби захисту інформації у телекомунікаційних системах**	Лекція / *Face to face*	Презентація	[12,19,21, 26] – відповідні теми	Опрацювати матеріал лекції. Самостійно опрацювати матеріал: Класифікація алгоритмів 2 год.	4	Самостійна робота до кінця 4 тижня
Тиж. 4	***Лабораторна робота №1. Аналіз***	Лабораторна	Методичні	[17,18,24] –	Оформити звіт з виконаної	6	Самостійна робота

(за розкладом) 2 год.	***антивірусних програм. Огляд апаратно-програмних пристроїв захисту інформації***	робота / *Face to face*	рекомендації	відповідні теми	лабораторної роботи та підготувати відповіді на контрольні питання. 2 год.		до кінця 4 тижня
Тиж. 5 (за розкладом) 2 год.	**Л3** **Апаратні та апаратно-програмні методи та засоби захисту інформації у телекомунікаційних системах**	Лекція / *Face to face*	Презентація	[17,18,24] – відповідні теми	Опрацювати матеріал лекції. Самостійно опрацювати матеріал: Класифікація методів захисту, апаратні методи 2 год.	4	Самостійна робота до кінця 6 тижня
Тиж. 6 (за розкладом) 2 год.	***Лабораторна робота №2_1. Аналіз вразливості, розробка модель зловмисника***	Лабораторна робота / *Face to face*	Методичні рекомендації	[18-20] – відповідні теми	Оформити звіт з виконаної лабораторної роботи та підготувати відповіді на контрольні питання. 2 год.	5	Самостійна робота до кінця 6 тижня
Тиж. 7 (за розкладом) 2 год.	**Л4** **Аналіз структури інформаційно-телекомунікаційної системи. Модель зловмисника. Ризики**	Лекція / *Face to face*	Презентація	[18-21] – відповідні теми	Опрацювати матеріал лекції. Самостійно опрацювати матеріал: Поняття моделі зловмисника, способи оцінки ризиків 2 год.	4	Самостійна робота до кінця 8 тижня
Тиж. 8 (за розкладом) 2 год.	***Лабораторна робота №2_2. Оцінка ризиків. Рекомендації вдосконалення системи інформаційного захисту***	Лабораторна робота / *Face to face*	Методичні рекомендації	[10,11,13] – відповідні теми	Оформити звіт з виконаної лабораторної роботи та підготувати відповіді на контрольні питання. 2 год.	5	Самостійна робота до кінця 8 тижня
Максимальна кількість балів за змістовим модулем 1						**36 балів**	
Модуль 2. Захист інформації у спеціальних інформаційно-телекомунікаційних системах							
Тиж. 9 (за розкладом) 2 год.	**Л5** **Технічний захист інформації в спеціальних ІТС**	Лекція / *Face to face*	Презентація	[24,25] – відповідні теми	Опрацювати матеріал лекції. Самостійно опрацювати матеріал: Засоби технічного захисту, сфера застосування інф. джерела: 2, 4. 2 год.	4	Самостійна робота до кінця 10 тижня
Тиж. 10 (за розкладом) 2 год.	***Лабораторна робота №3. Характеристика обраного технічного засобу ЗІ***	Лабораторна робота / *Face to face*	Методичні рекомендації	[24,25] – відповідні теми	Оформити звіт з виконаної лабораторної роботи та підготувати відповіді на контрольні питання. 2 год.	6	Самостійна робота до кінця 10 тижня
Тиж. 11 (за розкладом) 2 год.	**Л6** **Криптографічні методи захисту інформації при її передаванні у телекомунікаційних мережах**	Лекція / *Face to face*	Презентація	[16, 19, 20] – відповідні теми	Опрацювати матеріал лекції. Самостійно опрацювати матеріал: Особливості реалізації симетричних і асиметричних алгоритмів інф. джерела: 2, 4. 2 год.	4	Самостійна робота до кінця 12 тижня

Тиж. 12 (за розкладом) 2 год.	***Лабораторна робота №4. Програмна реалізація алгоритмів шифрування***	Лабораторна робота / *Face to face*	Методичні рекомендації	[10,11,13] – відповідні теми	Оформити звіт з виконаної лабораторної роботи та підготувати відповіді на контрольні питання. 2 год.	8	Самостійна робота до кінця 12 тижня
Тиж. 13 (за розкладом) 2 год.	**Л7 Стеганографічні методи захисту інформації при її передаванні у телекомунікаційних мережах**	Лекція / *Face to face*	Презентація	[15, 22] – відповідні теми	Опрацювати матеріал лекції. Самостійно опрацювати матеріал: інф. джерела: 2, 7, 11. 2 год.	4	Самостійна робота до кінця 14 тижня
Тиж. 14 (за розкладом) 2 год.	***Практична робота №2. Характеристика обраного стеганографічного методу: прихована передача, цифровий підпис***	Практична робота / *Face to face*	Методичні рекомендації	[15, 22] – відповідні теми	Оформити звіт з виконаної лабораторної роботи та підготувати відповіді на контрольні питання. 2 год.	8	Самостійна робота до кінця 14 тижня
Максимальна кількість балів за змістовим модулем 2						**34 балів**	
Максимальна кількість балів за екзамен						**30 балів**	
Максимальна кількість балів за курс						**100 балів**	

11. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю, усне опитування, письмовий контроль, тестовий контроль.

Форма підсумкового контролю: залік, екзамен.

Контроль знань і умінь (поточний і підсумковий) з дисципліни «Захист інформації в інформаційно – телекомунікаційних системах» здійснюється згідно з кредитною трансфернонакопичувальною системою організації навчального процесу. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою. Він складається з рейтингу навчальної роботи (засвоєння теоретичного матеріалу під час аудиторних занять та самостійної роботи, виконання лабораторних робіт та індивідуальних завдань), заліку у першому семестрі викладання дисципліни та екзамену у другому семестрі викладання дисципліни. В першому семестрі викладання дисципліни навчальна робота може бути оцінена максимум у 100 балів. У другому семестрі викладання дисципліни навчальна робота може бути максимум оцінена у 60 балів, на екзамені студент може добрати максимум 40 балів.

Розподіл балів, які отримують студенти при вивченні дисципліни «Захист інформації в інформаційно – телекомунікаційних системах»

<table>
<tr><td colspan="10">Поточний контроль та самостійна робота</td></tr>
<tr><td colspan="8">Модуль 1</td><td>Контроль</td><td>Сума</td></tr>
<tr><td colspan="2">Т1</td><td colspan="2">Т2</td><td colspan="2">Т3</td><td colspan="2">Т4</td><td rowspan="3">Звіти ЛР</td><td rowspan="3">36</td></tr>
<tr><td>Л</td><td>ПР1</td><td>Л</td><td>ЛР1</td><td>Л</td><td>ЛР1</td><td>Л</td><td>ЛР2</td></tr>
<tr><td>4</td><td>4</td><td>4</td><td>3</td><td>4</td><td>3</td><td>4</td><td>10</td></tr>
<tr><td colspan="8">Модуль 2</td><td>Контроль</td><td>Сума</td></tr>
<tr><td colspan="2">Т5</td><td colspan="2">Т6</td><td colspan="2">Т7</td><td colspan="2"></td><td rowspan="3">Звіти ЛР</td><td rowspan="3">34</td></tr>
<tr><td>Л</td><td>ЛР3</td><td>Л</td><td>ЛР4</td><td>Л</td><td>ПР2</td><td></td><td></td></tr>
<tr><td>4</td><td>6</td><td>4</td><td>8</td><td>4</td><td>8</td><td></td><td></td></tr>
<tr><td colspan="8"></td><td>іспит</td><td>30</td></tr>
<tr><td colspan="8">Заг. сума балів</td><td></td><td>100</td></tr>
</table>

Примітка: Т1, Т2,…,Т7 – тема, Л – теоретичні (лекційні) заняття, ЛБ – лабораторні роботи, ПР – практичні роботи

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90-100	**A**	відмінно	зараховано
82-89	**B**	добре	
74-81	**C**		
64-73	**D**	задовільно	
60-63	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-34	**F**	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

Критерії оцінювання. Еквівалент оцінки в балах для кожної окремої теми може бути різний, загальну суму балів за тему визначено в навчально-методичній карті. Розподіл балів між видами занять (лекції, практичні заняття, самостійна робота) можливий шляхом спільного прийняття рішення викладача і студентів на першому занятті:

оцінку **«відмінно» (90-100 балів, А)** заслуговує студент, який:

- всебічно, систематично і глибоко володіє навчально-програмовим матеріалом;
- вміє самостійно виконувати завдання, передбачені програмою, використовує набуті знання і вміння у нестандартних ситуаціях;
- засвоїв основну і ознайомлений з додатковою літературою, яка рекомендована програмою;
- засвоїв взаємозв'язок основних понять дисципліни та усвідомлює їх значення для професії, яку він набуває;
- вільно висловлює власні думки, самостійно оцінює різноманітні життєві явища і факти, виявляючи особистісну позицію;
- самостійно визначає окремі цілі власної навчальної діяльності, виявив творчі здібності і використовує їх при вивченні навчальнопрограмового матеріалу, проявив нахил до наукової роботи.

оцінку **«добре» (82-89 балів, B)** – заслуговує студент, який:
- повністю опанував і вільно (самостійно) володіє навчально-програмовим матеріалом, в тому числі застосовує його на практиці, має системні знання достатньому обсязі відповідно до навчально-програмового матеріалу, аргументовано використовує їх у різних ситуаціях;
- має здатність до самостійного пошуку інформації, а також до аналізу, постановки і розв'язування проблем професійного спрямування;
- під час відповіді допустив деякі неточності, які самостійно виправляє, добирає переконливі аргументи на підтвердження вивченого матеріалу;

оцінку **«добре» (74-81 бал, C)** - заслуговує студент, який:
- в загальному роботу виконав, але відповідає на екзамені з певною кількістю помилок;
- вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати на практиці, контролювати власну діяльність;
- опанував навчально-програмовий матеріал, успішно виконав завдання, передбачені програмою, засвоїв основну літературу, яка рекомендована програмою; оцінку **«задовільно» (64-73 бали, D)** – заслуговує студент, який:
- знає основний навчально-програмовий матеріал в обсязі, необхідному для подальшого навчання і використання його у майбутній професії; - виконує завдання, але при рішенні допускає значну кількість помилок;
- ознайомлений з основною літературою, яка рекомендована програмою;
- допускає на заняттях чи екзамені помилки при виконанні завдань, але під керівництвом викладача знаходить шляхи їх усунення. оцінку **«задовільно» (60-63 бали, E)** – заслуговує студент, який:
- володіє основним навчально-програмовим матеріалом в обсязі, необхідному для подальшого навчання і використання його у майбутній професії, а виконання завдань задовольняє мінімальні критерії. Знання мають репродуктивний характер.

оцінка **«незадовільно» (35-59 балів, FX)** – виставляється студенту, який:
- виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.

оцінку **«незадовільно» (35 балів, F)** – виставляється студенту, який:
- володіє навчальним матеріалом тільки на рівні елементарного розпізнавання і відтворення окремих фактів або не володіє зовсім;
- допускає грубі помилки при виконанні завдань, передбачених програмою;
- не може продовжувати навчання і не готовий до професійної діяльності після закінчення університету без повторного вивчення даної дисципліни.

12. Рекомендована література

Нормативні акти та закони

1. Конституція України // Урядовий кур'єр, 13 липня 1996 р.
2. Закон України "Про основи національної безпеки України"//
Урядовий кур'єр, 30 липня 2003 р.
3. Закон України "Про державну таємницю" від 21.01.1994 // Відомості Верховної Ради України, 1994, № 16. – Ст. 93.
4. Закон України "Про інформацію" // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.
5. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 // Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2005 р.
6. Закон України "Про телекомунікації" від 18.11.2003 // Відомості Верховної Ради України, 2004, № 12. – Ст. 155, із змінами 2004 р.
7. Постанова Кабінету Міністрів України "Про затвердження Концепції технічного захисту інформації в Україні" від 08.10.1997 р.
8. Постанова Кабінету Міністрів України "Про затвердження Положення про технічний захист інформації в Україні" від 09.09.1994 р.
9. Постанова Кабінету міністрів України "Про затвердження Концепції технічного захисту інформації в Україні" № 1126 від 08.11.1997 р.
10. Наказ МВС України від 14.07.1998 р. "Про організацію і виконання робіт з технічного захисту інформації з обмеженим доступом в системі МВС України". – К., 1998.
11. Наказ МВС України № 059 від 14.06.98 р. "Про організацію та виконання робіт з технічного захисту інформації з обмеженим доступом в системі МВС України".

Базова

12. Рибальський О.В. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України / Рибальський О.В., Смаглюк В.М., Хахановський В.Г. – К.: НАВС, 2013. – 255 с.
13. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник в 2-х т. / В.В. Поповский, А.В. Персиков. – Харьков: ООО «Компания СМИТ», 2006. – 238 с. [1]. – 292 с. [2].
14. Рибальський О.В. Інформаційна безпека правоохоронних органів. Курс лекцій / О.В. Рибальський, В.Г. Хахановський, В.В. Шорошев, О.І. Грищенко, С.В. Сторожев, М.В. Кобець. – К.: НАВСУ, 2003. – 160 с.

Допоміжна

15. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко – К.: МК–Пресс", 2006. – 283 с.
16. С. Синх. Книга кодов. Тайная история кодов и их "взлома" / С. Синх. – К.: "Махаон", 2007. – 447 с.
17. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ "ПолігрофКонсалтинг", 2004. – 216 с.
18. Конахович Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов.– К.: "МК–Пресс", 2005. – 288 с.

19. Ленков С.В. Методы и средства защиты информации. В 2–х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко.– Под ред. В.А. Хорошко.–К.: Арий, 2008. – Том 1. Несанкционированное получение информации. – 464 с.
20. Ленков С.В. Методы и средства защиты информации. В 2–х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – Под ред. В.А. Хорошко. – К.: Арий, 2008. – Том 2. Информационная безопасность. – 344 с.
21. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.
22. Хорошко В.О. Основи комп'ютерної стеганографії / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця.: ВДТУ, 2003. – 142 с.
23. Коженевський С.Р. Термінологічний довідник з питань захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков. – К.: ДУІКТ, 2007. – 382 с.
24. Захист інформації в автоматизованих системах управління [Текст]: навч. посібник/ Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
25. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / укл.: Г. І. Ластівка, П. М. Шпатар – Чернівці: Чернівецький національний університет, 2018. – 252 с.
26. Смірнова Т.В., Якименко Н.М., Улічев О.С., Конопліцька-Слободенюк О.К., Смірнов С.А., «Дослідження лінійних перетворень запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Кібербезпека: освіта, наука, техніка. № 3(15). С. 85-92. 2022. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/337 (Фахове видання. Категорія «Б»)