МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МАТЕМАТИЧНИЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ЗАТВЕРДЖУЮ
Декан математичного факультету
_____ С. І. Гоменюк
«01» вересня 2023 р.

АЛГОРИТМИ ШИФРУВАННЯ ТА ЗАХИСТУ ДАНИХ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

підготовки магістра
денної (очної) форми здобуття освіти
спеціальності 126 Інформаційні системи та технології
освітня програма Інформаційні системи та штучний інтелект

Укладач: Зіновєєв І. В., к.фіз.-мат.н., доцент, завідувач кафедри загальної математики

Обговорено та ухвалено
на засіданні кафедри комп'ютерних наук
Протокол № 1 від «30» серпня 2023 р.
В.о. завідувача кафедри
_____ Г. М. Шило

Ухвалено науково-методичною радою
математичного факультету
Протокол № 1 від «31» серпня 2023 р.
Голова науково-методичної ради
факультету
_____ О. С. Пшенична

Погоджено
гарант освітньо-професійної програми
_____ Г. М. Шило

2023 рік

1. Опис навчальної дисципліни

<table>
<tr><th>1</th><th>2</th><th colspan="2">3</th></tr>
<tr><td rowspan="2">Галузь знань, спеціальність, освітня програма рівень вищої освіти</td><td rowspan="2">Нормативні показники для планування і розподілу дисципліни на змістові модулі</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>очна (денна) форма здобуття освіти</td><td>заочна (дистанційна) форма здобуття освіти</td></tr>
<tr><td rowspan="2">Галузь знань
12 Інформаційні технології</td><td rowspan="2">Кількість кредитів – 3</td><td colspan="2">Обов’язкова</td></tr>
<tr><td colspan="2">Цикл професійної підготовки</td></tr>
<tr><td rowspan="2">Спеціальність
126 Інформаційні системи та технології</td><td rowspan="2">Загальна кількість годин – 90</td><td colspan="2">Семестр:</td></tr>
<tr><td>1-й</td><td></td></tr>
<tr><td rowspan="5">Освітньо-професійна програма
Інформаційні системи та штучний інтелект</td><td rowspan="5">Змістових модулів – 4</td><td colspan="2">Лекції</td></tr>
<tr><td>10 год.</td><td></td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>20 год.</td><td></td></tr>
<tr><td rowspan="3">Рівень вищої освіти:
другий (магістерський)</td><td rowspan="3">Кількість поточних контрольних заходів – 12</td><td colspan="2">Самостійна робота</td></tr>
<tr><td>60 год.</td><td></td></tr>
<tr><td colspan="2">Вид підсумкового семестрового контролю: екзамен</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Курс «Алгоритми шифрування та захисту даних» є необхідною складовою частиною базової теоретичної та практичної підготовки студента, що навчається за освітньою програмою «Інформаційні системи та штучний інтелект», а також є основою для подальшого вивчення спеціальних дисциплін.

Курс «Алгоритми шифрування та захисту даних» складається з 4-х змістових модулів:

1. Основні поняття криптографії та захисту інформації. Історичний огляд криптографічних методів захисту інформації. Класичні алгоритми симетричного шифрування;
2. Симетрична та асиметрична криптографія. Класичні алгоритми асиметричного шифрування. Алгоритми на основі мереж Фейстеля та SP-мереж;
3. Сучасні криптографічні методи захисту інформації. Блокове шифрування. Основні принципи роботи блокових шифрів. Сучасні криптосистеми на основі блокового шифрування;

4. Алгоритми захисту даних. Електронний цифровий підпис. Алгоритми та технології аутентифікації.

Основною метою вивчення навчальної дисципліни «Алгоритми шифрування та захисту даних» є отримання здобувачами компетентностей в області криптографії, криптографічного захисту даних.

Основними **завданнями** курсу є:

- надання студентам теоретичних знань про задачі та особливості криптографічного захисту інформації;
- формування у студентів категоріальних понять з основ математики симетричної та асиметричної криптографії;
- формування у студентів умінь обчислювати параметри цифрового підпису і розподілу ключів на основі відомих протоколів;
- стимулювання студентів до активної аналітико-пошукової роботи;
- вдосконалення вміння щодо пошуку, добору й опрацюванню наукової інформації, точного формулювання мети, задач і висновків дослідження.

У разі успішного завершення курсу студент **зможе**:

- застосовувати на практиці набуті знання про джерела і способи дії загроз на об’єкти інформаційної безпеки ;
- використовувати фундаментальні та спеціальні знання з математики до розв’язання прикладних задач в галузі шифрування, кодування даних, захисту даних;
- володіти алгоритмами шифрування інформаційних текстів та застосовувати їх;
- працювати з концептуальними моделями розробки, розподілу, обробки, використання та зберігання конфіденціальних документів;
- створювати засобами стандартного програмного забезпечення елементи захисту даних.

Використання новітніх програмних засобів під час виконання практичних та лабораторних завдань розвине як загальні, так і професійні компетенції слухачів.

Згідно з вимогами освітньо-професійної програми студенти повинні досягти таких **результатів навчання (компетентностей)**:

Заплановані робочою програмою результати навчання та компетентності	**Методи і контрольні заходи, що забезпечують досягнення результатів навчання та компетентностей**
Результати навчання	
РН 1. Відшуковувати необхідну інформацію в науковій і технічній літературі, базах даних, інших джерелах, аналізувати та оцінювати цю інформацію	Методи навчання: пояснення, спостереження, лекція-візуалізація, лабораторні роботи, частково-пошуковий, дослідницький метод, індивідуальне і групове консультування. робота з літературою. Контрольні заходи: захист лабораторних робіт, опитування, тестування, реферат.

Заплановані робочою програмою результати навчання та компетентності	**Методи і контрольні заходи, що забезпечують досягнення результатів навчання та компетентностей**
РН 10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації	Методи навчання: лекція-візуалізація, лабораторні роботи, ілюстрація, демонстрація, пояснення, спостереження, майстер-клас, частково-пошуковий, дослідницький метод, робота з літературою, вправи, відеоконференції, індивідуальне і групове консультування, тестування, відеозаписи лекцій Контрольні заходи: захист лабораторних робіт, опитування, тестування, реферат.
РН 12. Розробляти та використовувати методи штучного інтелекту	Методи навчання: лекція-візуалізація, лабораторні роботи, ілюстрація, демонстрація, пояснення, спостереження, майстер-клас, частково-пошуковий, дослідницький метод, робота з літературою, вправи, відеоконференції, індивідуальне і групове консультування, тестування, відеозаписи лекцій Контрольні заходи: захист лабораторних робіт, опитування, тестування, реферат.
РН 13. Розробляти та використовувати алгоритми шифрування та захисту даних в інформаційних системах	Методи навчання: лекція-візуалізація, лабораторні роботи, ілюстрація, демонстрація, пояснення, спостереження, майстер-клас, частково-пошуковий, дослідницький метод, робота з літературою, вправи, відеоконференції, індивідуальне і групове консультування, тестування, відеозаписи лекцій Контрольні заходи: захист лабораторних робіт, опитування, тестування, реферат.
Компетентності	
ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу	Методи навчання: лекція-візуалізація, лабораторні роботи, ілюстрація, демонстрація, пояснення, спостереження, майстер-клас, частково-пошуковий, дослідницький метод, робота з літературою, вправи, відеоконференції, індивідуальне і групове консультування, тестування, відеозаписи лекцій Контрольні заходи: захист лабораторних робіт, опитування, тестування, реферат.
СК 4. Здатність розробляти математичні, інформаційні та комп'ютерні моделі об'єктів і процесів інформатизації	Методи навчання: лекція-візуалізація, лабораторні роботи, ілюстрація, демонстрація, пояснення, спостереження, майстер-клас, частково-пошуковий, дослідницький метод, робота з літературою, вправи, відеоконференції, індивідуальне і групове консультування, тестування, відеозаписи лекцій Контрольні заходи: захист лабораторних робіт, опитування, тестування, реферат.
СК 6. Здатність управляти інформаційними ризиками на основі	Методи навчання: лекція-візуалізація, лабораторні роботи, ілюстрація, демонстрація, пояснення, спостереження, майстер-клас, частково-пошуковий,

Заплановані робочою програмою результати навчання та компетентності	Методи і контрольні заходи, що забезпечують досягнення результатів навчання та компетентностей
концепції інформаційної безпеки	дослідницький метод, робота з літературою, вправи, відеоконференції, індивідуальне і групове консультування, тестування, відеозаписи лекцій Контрольні заходи: захист лабораторних робіт, опитування, тестування, реферат.
СК 10. Здатність застосовувати методи захисту даних в інформаційних системах	Методи навчання: лекція-візуалізація, лабораторні роботи, ілюстрація, демонстрація, пояснення, спостереження, майстер-клас, частково-пошуковий, дослідницький метод, робота з літературою, вправи, відеоконференції, індивідуальне і групове консультування, тестування, відеозаписи лекцій Контрольні заходи: захист лабораторних робіт, опитування, тестування, реферат.

Міждисциплінарні зв'язки. Знання отримані при вивченні дисципліни «Алгоритми шифрування та захисту даних» можуть бути використані при опанування курсів «Організація баз даних і баз знань», «Проєктування інформаційних систем», а також можуть слугувати підготовчою базою для проходження виробничої практики, виконання кваліфікаційної роботи.

3. Програма навчальної дисципліни

Змістовий модуль 1. Основні поняття криптографії та захисту інформації.

Історія криптографії. Криптографія та захист даних. Поняття та види шифрів. Вимоги до шифрів - принцип Керхгоффа. Шифрувальні машини. Ідеальний шифр і класи стійкості шифрів. Класичні алгоритми симетричного шифрування.;

Змістовий модуль 2. Симетрична та асиметрична криптографія.

Класичні алгоритми симетричного та асиметричного шифрування. Шифри заміни. Шифри переставляння. Шифри гамування. Мережа Фейстеля. Шифри на основі мережі Фейстеля. Американський шифр DES. Шифри на основі SP-мережі.

Змістовий модуль 3. Сучасні криптографічні методи захисту інформації, основні види та їх реалізація.

Блокове шифрування. Основні принципи роботи блокових шифрів. Сучасні криптосистеми на основі блокового шифрування. (ДСТУ 28147:2009, DES, AES, Rijndael, ДСТУ 7624:2014 «Калина»).

Складені шифри

Змістовий модуль 4. Алгоритми захисту даних. Електронний цифровий підпис (ЦП). Стандарти ЦП. Цифровий підпис RSA.

Алгоритми та технології аутентифікації Системи захисту Діффі-Хеллмана. Криптосистема Ель–Гамаля.

4. Структура навчальної дисципліни

Зміст. модуль	Усього годин	Аудиторні (контактні) години			Самостійна робота, год	Система накопичення балів		
		Усього годин	Лекційні заняття, год.	Лабораторні заняття, год.		Теор. завд., к-ть балів	Практ.. завд., к-ть балів	Усього балів
1	**2**	**3**	**5**	**7**	**9**	**11**	**12**	**13**
1	15	6	2	4	9	4	8	12
2	15	9	2	6	7	6	12	18
3	15	9	4	6	5	6	12	18
4	15	6	2	4	9	4	8	12
Усього за зміст. модулі	**60**	**30**	**10**	**20**	**30**	**20**	**40**	**60**
Підсумковий семестровий контроль **ІДЗ**	**15**				**15**	**10**	**10**	**20**
Підсумковий семестровий контроль **екзамен**	**15**				**15**	**10**	**10**	**20**
Загалом	**90**	**30**	**10**	**20**	**60**	**40**	**60**	**100**

5. Теми лекційних занять

№ зміст. модуля	Назва теми	Кільк-ть годин
1	Основні поняття криптографії та захисту інфор-мації. Історія криптографії. Криптографія та захист даних. Поняття та види шифрів. Вимоги до шифрів - принцип Керхгоффа. Шифрувальні машини. Ідеальний шифр і класи стійкості шифрів. Класичні алгоритми симетричного шифрування.	2
2	Симетрична та асиметрична криптографія. Класичні алгоритми симетричного та асиметричного шифрування. Шифри заміни. Шифри переставляння. Шифри гамування.	2
3	Сучасні криптографічні методи захисту інформації, основні види та їх реалізація. Мережа Фейстеля. Шифри на основі мережі Фейстеля. Американський шифр DES. Шифри на основі SP-мережі.	2
3	Блокове шифрування. Основні принципи роботи блокових шифрів. Сучасні криптосистеми на основі блокового шифру-вання. (ДСТУ 28147:2009, DES, AES, , Rijndael, ДСТУ 7624:2014 «Калина»). Складені шифри	2
4	Алгоритми захисту даних. Електронний цифровий підпис (ЦП). Стандарти ЦП. Цифровий підпис RSA. Алгоритми та технології аутентифікації Системи захисту Діффі-Хеллмана. Криптосистема Ель–Гамаля.	2
	Разом	**10**

6. Теми лабораторних занять

№ зміст. модуля	Назва теми	Кільк-ть годин
1	Класичні алгоритми симетричного та асиметричного шифрування. Шифр Цезаря. Квадрати Полібія. Шифри заміни.	2
	Класичні алгоритми симетричного та асиметричного шифрування. Шифр Кардано. Шифри переставляння.	2
2	Класичні алгоритми симетричного та асиметричного шифрування. Шифри гамування.	2
	Класичні алгоритми симетричного та асиметричного шифрування. Мережа Фейстеля.	2
	Класичні алгоритми симетричного та асиметричного шифрування. Шифри на основі SP-мережі.	2
3	Блокове шифрування. ДСТУ 28147:2009.	2
	Блокове шифрування. AES. Американський шифр DES.	2
	Блокове шифрування. ДСТУ 7624:2014 «Калина».	2
4	Алгоритми захисту даних. Електронний цифровий підпис (ЦП). Цифровий підпис RSA.	2
	Алгоритми та технології аутентифікації Системи захисту Діффі-Хеллмана. Алгоритми та технології аутентифікації Криптосистема Ель–Гамаля.	2
	Разом	**20**

7. Види і зміст поточних контрольних заходів

Поточні контрольні заходи

Теоретичний контроль (кількість балів зазначено на сторінці дисципліни в moodle) – усні та письмові (до 3балів за поточний контроль) опитування на лекціях, лабораторних заняттях, тестування (до 5б. за тест поточного контролю).

Практичний контроль (кількість балів зазначено на сторінці дисципліни в moodle) – розв'язання практичних завдань, виконання лабораторних робіт, завдань самостійної роботи (до 5 балів за один контроль), письмові контрольні роботи (до 5 балів за один контроль, двічі на семестр), тестування – (до 5 балів за тест).

Реферат – оволодіння матеріалом, що виноситься на самостійну роботу (до 3 балів за один реферат, двічі на семестр).

Підсумкові контрольні заходи:

Індивідуальне дослідницьке завдання, проект (ІДЗ, можливо виконання у групі з двох, трьох студентів).

ІДЗ видається за один – два місяці до завершення теоретичного навчання поточного семестру. Термін виконання не менше одного місяця. Виконане ІДЗ, на передостанньому тижні теоретичного навчання поточного семестру подається викладачеві у вигляді оформленої пояснювальної записки

(постановка задачі, побудова та обґрунтування адекватності обраної математичної моделі, криптосистеми, обґрунтування методу розв'язання поставленої задачі, розв'язок задачі, інтерпретація отриманих результатів, рекомендації до застосування).

На останньому тижні проводиться публічний захист у групі (до 20 балів).

Формат захисту ІДЗ проекту: презентація, тривалістю до 10 хвилин та відповідь на задані присутніми питання (до 5 хвилин).

Детальні вимоги та практичні рекомендації до виконання ІДЗ на сторінці курсу у Moodle та на поточних консультаціях.

Залікове тестове завдання (до 20 балів)– проводиться у системі Moodle або MyTestXPro із використанням (за необхідністю) розроблених програмних продуктів, та спеціального програмного забезпечення. Критерії оцінювання та вимоги до тесту наведено в інструкції до тесту та поточній консультації.

№ змістового модуля	Вид поточного контрольного заходу	Зміст поточного контрольного заходу	Критерії оцінювання	Усього балів
1	Захист лабораторної роботи №1	Перевірка оволодіння теоретичним матеріалом, що відповідає змісту завдань лабораторної роботи. Захист виконаних завдань лабораторної роботи, перевірка оволодіння практичними вміннями та навичками.	Правильні відповіді – 1 бал Повне виконання завдань Л/Р з оформленням звіту у відповідності до вимог – 4 бали	**5**
	Захист лабораторної роботи №2	Перевірка оволодіння теоретичним матеріалом, що відповідає змісту завдань лабораторної роботи. Захист виконаних завдань лабораторної роботи, перевірка оволодіння практичними вміннями та навичками.	Правильні відповіді – 1 бал Повне виконання завдань Л/Р з оформленням звіту у відповідності до вимог – 4 бали	**5**
	Тестування	Перевірка оволодіння теоретичним матеріалом, практичними вміннями та навичками	Оцінювання завдань згідно з інструкцією до тестових завдань	**2**
2	Захист лабораторної роботи №3	Перевірка оволодіння теоретичним матеріалом, що відповідає змісту завдань лабораторної роботи. Захист виконаних завдань лабораторної роботи, перевірка оволодіння практичними вміннями та навичками.	Правильні відповіді – 1 бал Повне виконання завдань Л/Р з оформленням звіту у відповідності до вимог – 4 бали	**5**
	Захист лабораторної роботи №4	Перевірка оволодіння теоретичним матеріалом, що відповідає змісту завдань лабораторної роботи. Захист виконаних завдань лабораторної роботи, перевірка оволодіння практичними вміннями та навичками.	Правильні відповіді – 1 бал Повне виконання завдань Л/Р з оформленням звіту у відповідності до вимог – 4 бали	**5**
	Захист лабораторної	Перевірка оволодіння теоретичним матеріалом, що відповідає змісту завдань лабораторної роботи.	Правильні відповіді – 1 бал	**5**

№ змістового модуля	Вид поточного контрольного заходу	Зміст поточного контрольного заходу	Критерії оцінювання	Усього балів
	роботи №5	Захист виконаних завдань лабораторної роботи, перевірка оволодіння практичними вміннями та навичками.	Повне виконання завдань Л/Р з оформленням звіту у відповідності до вимог – 4 бали	
	Тестування	Перевірка оволодіння теоретичним матеріалом, практичними вміннями та навичками.	Оцінювання завдань згідно з інструкцією до тестових завдань	**3**
3	Захист лабораторної роботи №6	Перевірка оволодіння теоретичним матеріалом, що відповідає змісту завдань лабораторної роботи. Захист виконаних завдань лабораторної роботи, перевірка оволодіння практичними вміннями та навичками.	Правильні відповіді – 1 бал Повне виконання завдань Л/Р з оформленням звіту у відповідності до вимог – 4 бали	**5**
	Захист лабораторної роботи №7	Перевірка оволодіння теоретичним матеріалом, що відповідає змісту завдань лабораторної роботи. Захист виконаних завдань лабораторної роботи, перевірка оволодіння практичними вміннями та навичками.	Правильні відповіді – 1 бал Повне виконання завдань Л/Р з оформленням звіту у відповідності до вимог – 4 бали	**5**
	Захист лабораторної роботи №8	Перевірка оволодіння теоретичним матеріалом, що відповідає змісту завдань лабораторної роботи. Захист виконаних завдань лабораторної роботи, перевірка оволодіння практичними вміннями та навичками.	Правильні відповіді – 1 бал Повне виконання завдань Л/Р з оформленням звіту у відповідності до вимог – 4 бали	**5**
	Тестування	Перевірка оволодіння теоретичним матеріалом, практичними вміннями та навичками.	Оцінювання завдань згідно з інструкцією до тестових завдань	**3**
4	Захист лабораторної	Перевірка оволодіння теоретичним матеріалом, що відповідає змісту завдань лабораторної роботи.	Правильні відповіді – 1 бал	**5**

№ змістового модуля	Вид поточного контрольного заходу	Зміст поточного контрольного заходу	Критерії оцінювання	Усього балів
	роботи №9	Захист виконаних завдань лабораторної роботи, перевірка оволодіння практичними вміннями та навичками.	Повне виконання завдань Л/Р з оформленням звіту у відповідності до вимог – 4 бали	
	Захист лабораторної роботи №10	Перевірка оволодіння теоретичним матеріалом, що відповідає змісту завдань лабораторної роботи. Захист виконаних завдань лабораторної роботи, перевірка оволодіння практичними вміннями та навичками.	Правильні відповіді – 1 бал Повне виконання завдань Л/Р з оформленням звіту у відповідності до вимог – 4 бали	**5**
	Тестування	Перевірка оволодіння теоретичним матеріалом, практичними вміннями та навичками	Оцінювання завдань згідно з інструкцією до тестових завдань	**2**
Усього				**60**

8. Підсумковий семестровий контроль

Форма	Види підсумкових контрольних заходів	Зміст підсумкового контрольного заходу	Критерії оцінювання	Усього балів
Екзамен	Підсумковий тест в СЕЗН ЗНУ Moodle	Тест складається з теоретичних (тестові питання різного типу) та практичних завдань (відкритий та закритий тип, есе з наданням короткої або розгорнутої відповіді)	Оцінювання завдань згідно з інструкцією до тестових завдань	**20**

9. Рекомендована література

ОСНОВНА

1. Євсеєв С. П., Мілов О. В., Король О. Г. Лабораторний практикум з основ криптографічного захисту : навч. посіб. Харків : ХНЕУ ім. С. Кузнеця, 2020. 222 с.
2. Інформаційна безпека : навч. посібник / Ю. Я. Бобало та ін. Львів : Видавництво Львівської політехніки, 2019. 580 с.
3. Козіна Г. Л. Криптографія від історії до сучасних стандартів: навч.посібник. Запоріжжя : НУ «Запорізька політехніка», 2020. 192 с.
4. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології». Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.
5. Jean-Philippe Aumasson. Serious Cryptography: A Practical Introduction to Modern Encryption Paperback. Kindle Edition, 2017. 313 p.
6. Klima, R.E., Klima, R., Sigmon, N.P., & Sigmon, N. (2018). Cryptology: Classical and Modern (2nd ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781315170664
7. Steinberg J., Beaver K., Winkler I., Coombs T. Cybersecurity All-in-One For Dummies. New York: Wiley, 2022. 700 p.

ДОДАТКОВА

1. Вербівський Д., Якимчук Б. Криптологія: опорний коспект лекцій. Житомир: Вид-во ЖДУ ім. Івана Франка, 2023. 173 с.
2. Глинчук Л.Я. Криптологія : навч.-метод. посіб. Луцьк: Вежа-Друк, 2014. 164 с.
3. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія: Теорія. Практика. Застосування. Харків : Форт, 2013. 880 с.
4. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посіб. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
5. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Чинний від 2015–07–01] Вид. офіц. Київ : Мінекономрозвитку України, 2015. (Інформація та документація)
6. Методичні рекомендації до виконання лабораторних робіт з дисципліни "Прикладна криптологія": (Для студентів техн. спец. вищ. навч. закл.) / А.Д. Кожухівський та ін.. – Київ: Державний університет телекомунікацій, 2020. 109 с. URL: https://dut.edu.ua/uploads/l_2167_57004775.pdf (дата звернення: 15.08.2023)
7. Полторак В. П., Савчук О. В. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах. Вибрані розділи : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології». Київ : КПІ ім. Ігоря Сікорського, 2021. 385с.

Інформаційні ресурси

1. Законодавство України. Офіційний сайт парламенту України. URL: http://zakon.rada.gov.ua.
2. Платформа підвищення кваліфікації з кібербезпеки. URL: https://www.rangeforce.com.
3. Портал безкоштовних програм електронного навчання в галузі криптографії та криптоаналізу The CrypTool Portal. URL: http://www.cryptool.org/en.
4. Сайт Національної академії внутрішніх справ України. URL: http://www.naiau.kiev.ua.
5. Сайт повної та безкоштовної реалізації стандарту GNU Privacy Guard OpenPGP. URL: http://www.gnupg.org GnuPG.
6. Сайт розробника алгоритму і програми PGP. URL: http://www.pgpi.com.
7. Український ресурс з безпеки. URL: http://kiev-security.org.ua.
8. Центр комп'ютерної безпеки м. Київ. URL: https://infocity.kiev.ua.