МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Центральноукраїнський державний педагогічний університет імені Володимира Винниченка

Кафедра математики, статистики та інформаційних технологій

«ЗАТВЕРДЖУЮ»

Завідувач кафедри

Авраменко О.В. _____

7 вересня 2021 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації

Спеціальність: 014.09 Середня освіта (Інформатика)

Освітні програми: Середня освіта (Інформатика та Математика)

факультет математики, природничих наук та технологій

форма навчання денна

2021 – 2022 навчальний рік

Робоча програма «Захист інформації» для студентів за спеціальністю 014.09 Середня освіта (Інформатика)

Розробник: Пузікова А.В. – кандидат фізико-математичних наук, доцент, старший викладач кафедри математики, статистики та інформаційних технологій

Робочу програму схвалено на засіданні кафедри математики, статистики та інформаційних технологій Центральноукраїнського державного педагогічного університету імені Володимира Винниченка

Протокол від “7” вересня 2021 року № 1

Завідувач кафедри математики, статистики
та інформаційних технологій _____ (проф. Авраменко О.В.)

1. **Опис навчальної дисципліни**

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність/напрям, рівень вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 3</td><td>Галузь знань
01 Освіта/Педагогіка</td><td colspan="2">обов’язковий компонент ОПП</td></tr>
<tr><td rowspan="2">Індивідуальне науково-дослідне завдання _____</td><td rowspan="4">014.09 Середня освіта (Інформатика)
(друга спеціальність – 014.04 Середня освіта (Математика))</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>4-й</td><td>-й</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 90:</td><td colspan="2">Семестри</td></tr>
<tr><td>7-й</td><td>-й</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:

аудиторних – 2
самостійної роботи студента – 3</td><td rowspan="10">Рівень вищої освіти: бакалавр</td><td colspan="2">Лекції</td></tr>
<tr><td>20 год.</td><td>год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>16 год.</td><td>год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>54 год.</td><td>год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання: год.</td></tr>
<tr><td>Вид контролю:</td><td></td></tr>
<tr><td>екзамен</td><td></td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Мета курсу «Захист інформації» – забезпечення фундаментальної теоретичної і практичної підготовки бакалаврів для набуття ними концептуальних наукових та практичних знань з питань захисту комп’ютерних систем від несанкціонованого доступу, основних методів захисту ПЗ, організації захисту в інформаційно-комунікаційних системах, криптографії та криптоаналізу, вміння застосовувати ці знання у сфері професійної педагогічної діяльності.

Завдання. Оволодіти теоретичними і практичними основами використання основних методів захисту інформації.

У результаті вивчення дисципліни «Захист інформації» у студента мають бути сформовані такі *компетентності:*

- Інтегральна компетентність. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі освіти та інформатики, що передбачає застосування певних теорій і методів педагогічних та комп’ютерних наук і характеризується комплексністю та невизначеністю умов.
- ЗК.02. Здатність до міжособистісної взаємодії, роботи в команді.
- ЗК.04. Здатність до прийняття ефективних рішень у професійній діяльності та відповідального ставлення до обов’язків, мотивування людей до досягнення спільної мети.
- ФК01. Здатність до формування в учнів ключових і предметних компетентностей та здійснення міжпредметних зв’язків; здатність здійснювати інтегроване навчання учнів.
- ПК01. Здатність використовувати знання наукових фактів, концепцій, теорій, принципів, методів інформатики та математики у практиці навчання цих дисциплін у базовій середній школі.

- ПК03. Здатність розробляти, досліджувати, реалізовувати мовами програмування алгоритми розв’язання задач з інформатики.
- ПК04. Здатність використовувати програмні засоби загального та спеціального призначення для розв’язання прикладних задач з інформатики.
- ПК.05. Володіння технологіями налагодження, обслуговування та експлуатації комп’ютерної мережі; здатність реалізовувати комплекс заходів, спрямованих на забезпечення захищеності інформації, здатність формувати вміння безпечної роботи школярів у комп’ютерній мережі.

Програмні результати навчання:

- ПРН.16. Знання фізичних, логічних та математичних основ інформаційних технологій. Уміння використовувати цифрові пристрої, їх програмне забезпечення; працювати з операційними системами, онлайн-сервісами, застосунками, мережею інтернет, хмарними технологіями.
- ПРН.17. Знання способів двійкового кодування текстових, числових, графічних, звукових та відео даних. Уміння використовувати інформаційно-комунікаційні технології для подання, редагування, збереження та перетворення зазначених типів даних.
- ПРН.18. Знання принципів функціонування та основ архітектури комп’ютерних систем та мереж; уміння впроваджувати засоби й методи захисту інформації та безпеки в мережі інтернет.

3. Тематичний план навчальної дисципліни

Розділ 1. Загальні поняття та положення із захисту інформації. Класичні криптографічні засоби шифрування.

Тема 1. Загальні поняття та положення із захисту інформації. Значення інформації і її захисту. Носії інформації і їх захист.

Тема 2. Криптографія стародавнього світу.

1. Атбаш, шифр скитала, шифр частоколу.
2. Шифри простої заміни. Шифр зсуву. Шифр Цезаря.
3. Криптоаналіз шифру простої заміни.

Тема 3. Криптографія середніх віків.

1. Решітка Кардано. Шифр Бекона.
2. Шифр Віженера. Шифр з автоключем.
3. Метод гамування.
4. Поліалфавітні підстановки.
5. Гомофонний шифр заміни Гауса.
6. Поліграмні шифри.
7. Шифри перестановки. Матричний шифр обходу.
8. Криптоаналіз шифрів перестановки.

Тема 4. Криптографія Нового часу.

1. Роторні шифрувальні машини.
2. Потокові шифри. Шифр одноразового блокноту.
3. Умова абсолютної стійкості шифру за Шеноном.
4. Генератори псевдовипадкових бітів. Генератори на регістрах зсуву з лінійним зворотним зв’язком.

Тема 5. Математичні основи сучасної криптографії.

1. Шифр Хілла.
2. Лінійний шифр.
3. Афінний шифр.

4. Афінні шифри вищих порядків.
5. Криптоаналіз шифрів к-го порядку з відомим відкритим текстом.

Розділ 2. Стандарти шифрування даних.

Тема 6. Симетричні криптосистеми.

1. Поняття криптосистеми. Класифікація криптографічних систем.
2. Криптосистеми з симетричними ключами та їх властивості. Принцип Керкгофа стійкості криптосистем.
3. Мережі Фейстеля.
4. Стандарт блокового симетричного шифрування даних DES. Формування ключа. Схема розшифрування. Криптостійкість.

Тема 7. Асиметричні криптосистеми.

1. Поняття однобічної функції.
2. Ранцеві криптосистеми.
   - Задача про ранець в криптографії. Задача про ранець з надзростаючим вектором.
   - Алгоритм Меркла-Хеллмана.
3. Модель криптосистеми з публічними ключами.
4. Алгоритм RSA.
5. Алгоритм шифрування сеансового ключа.
6. Цифровий підпис.
7. Способи зламу системи RSA.

Тема 8. Стеганографія.

1. Стеганографічні системи
   - Сфери застосування стеганографії.
   - Атаки на стеганографічні системи та протидія їм.
2. Методи стенографії
   - Приховування даних у нерухомих цифрових зображеннях, відеофайлах та аудіофайлах.
   - Текстова стенографія.

Тема 9. Ідентифікація. автентифікація. санкціонований доступ**.**

1. Автентифікація
   - Основні визначення (термінологія).
   - Ідентифікація та автентифікація об’єктів.
   - Системи захисту цілісності даних.
   - Задачі автентифікації.
   - Криптографічні хеш-функції та їх застосування в криптографії.

Розділ 3. Атаки, поняття та методи захисту.

Тема 10. Аналіз атак

1. Типи зловмисного ПЗ
   - Шпигунські програми (Spyware).
   - Рекламне ПЗ (Adware).
   - Бот (Bot).
   - Програми-вимагачі (Ransomware).
   - Псевдоантивірус (Scareware).
   - Руткіт (Rootkit).
   - Вірус (Virus).
   - Троянський кінь (Trojan horse).
   - Черв'яки або хробаки (Worms).
   - Людина посередині (Man-In-The-Middle або MitM).

- Посередник в мобільному телефоні (Man-In-The-Mobile або MitMo).

2. Методи проникнення
   - соціальна інженерія;
   - атаки грубої сили (Brute-force attacks);
   - прослуховування мережі (Network sniffing);
   - фішинг;
   - використання вразливостей.
3. DoS, DDoS та SEO-атаки.

Тема 11. Методи захисту даних, пристроїв і мережі**.**

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	денна форма					
	усього	у тому числі				
		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7
Розділ 1. *Загальні поняття та положення із захисту інформації. Класичні криптографічні засоби шифрування*						
Тема 1. Загальні поняття та положення із захисту інформації. Значення інформації і її захисту. Носії інформації і їх захист.	4	1				3
Тема 2. Криптографія стародавнього світу.	7	1		2		4
Тема 3. Криптографія середніх віків.	9	2		2		5
Тема 4. Криптографія Нового часу.	9	2		2		5
Тема 5. Математичні основи сучасної криптографії.	10	2		2		6
Розділ 2. *Стандарти шифрування даних*						
Тема 6. Симетричні криптосистеми.	9	2		2		5
Тема 7. Асиметричні криптосистеми.	11	4		2		5
Тема 8. Стеганографія.	7	1		2		4
Тема 9. Ідентифікація. Автентифікація. Санкціонований доступ**.**	5	1				4
Розділ 3. *Атаки, поняття та методи захисту.*						
Тема 10. Аналіз атак**.**	8	2				6
Тема 11. Методи захисту даних, пристроїв і мережі**.**	11	2		2		7
Усього годин	**90**	**20**		**16**		**54**

5. Теми семінарських (практичних) занять

№ з/п	Назва теми	Кількість годин
1	Не передбачено	

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	**Тема 2.** Криптографія стародавнього світу.	2
2.	**Тема 3.** Криптографія середніх віків.	2
3.	**Тема 4.** Криптографія Нового часу.	2
4.	**Тема 5.** Математичні основи сучасної криптографії.	2
5.	**Тема 6.** Симетричні криптосистеми.	2
6.	**Тема 7**. Асиметричні криптосистеми.	2
7.	**Тема 8**. Стеганографія.	2
8.	**Тема 11**. Методи захисту даних, пристроїв і мережі.	2
Разом		**16**

7. Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин
1.	**Тема 1**. Загальні поняття та положення із захисту інформації. Значення інформації і її захисту. Носії інформації і їх захист.	3
9.	**Тема 2.** Криптографія стародавнього світу.	4
10.	**Тема 3.** Криптографія середніх віків.	5
11.	**Тема 4.** Криптографія Нового часу.	5
12.	**Тема 5.** Математичні основи сучасної криптографії.	6
13.	**Тема 6.** Симетричні криптосистеми.	5
14.	**Тема 7**. Асиметричні криптосистеми.	5
15.	**Тема 8**. Стеганографія.	4
16.	**Тема 9**. Методи захисту даних, пристроїв і мережі.	4
2.	**Тема 10**. Аналіз атак**.**	6
3.	**Тема 11**. Методи захисту даних, пристроїв і мережі**.**	7
Разом		**54**

8. Індивідуальні завдання

9. Викладання та навчання

Викладання проводиться у вигляді лекцій (у т.ч. мультимедійні та інтерактивні лекції), лабораторних робіт дослідницького характеру, самостійної роботи на основі електронних навчальних комплексів, консультацій із викладачами.

10. Методи контролю

- усний і лабораторний контроль (індивідуальне опитування при захисті лабораторної роботи);
- письмовий контроль (самостійні та контрольні роботи, письмові заліки й екзамени);
- тестування.

11. Схема нарахування балів, які отримують студенти

Оцінювання навчальних досягнень здійснюється за 100-бальною (рейтинговою) шкалою ЕКТС (ECTS), національною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно») і вербальною («зараховано», «не зараховано») системами.

Визначення вагових балів (ціле число) з кожного контрольного заходу (R_K) на підставі розподілу навчального часу студентів згідно з тематичним планом робочої програми кредитного модуля здійснюється за формулою:

$$R_k = R\frac{t_k}{\sum t_i}, \text{ де}$$

t_k – навчальний час, запланований у робочій програмі для засвоєння навчального матеріалу та досягнення певних результатів навчання (знань і умінь), які мають контролюватися k-м контрольним заходом;

$\sum t_i$ – загальний навчальний час, призначений для засвоєння навчального матеріалу, який охоплюється всіма контрольними заходами;

R – значення розміру шкали (100 балів для заліку, 60 балів для екзамену).

Екзамен (7 семестр)

Розподіл балів, які отримують студенти

	Розділ 1					Розділ 2				Розділ 3		Сума
	Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	
Поточний контроль		5	5	5	5	5	5	5			5	40
Самостійна робота	10											10
Контрольна робота	10											10
Екзамен												40
Разом												100

Т1, Т2 ... Т11 – теми розділів.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	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
0-34	**F**	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

12. Рекомендована література

Основна

1. Інформаційна безпека: навч. посібн. / Ю.Я. Бобайло, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв, С.С.Войтусік, А.Я. Горпенюк, О.А. Нємкова, І.М. Журавель, Б.М. Березюк, Є.І. Яковенко, В.І. Отенко, І.Я. Тишик. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
2. Грайворонський М.В. Безпека інформаційно-комунікаційних систем. / Грайворонський М.В., Новіков О.М. – К.: Видавнича група BHV, 2009. – 608 с.
3. 3. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
4. 4. Технології захисту інформації [Електронний ресурс] : / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
5. Лужецький В. А. Основи інформаційної безпеки : навч. посіб. / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця : ВНТУ, 2013. – 221 с.

Допоміжна

6. Сенів М. М., Яковина В. С. Безпека програм та даних. Навчальний посібник. Львів : Видавництво Львівської політехніки, 2015.
7. Чігірьов С.П. Методи автентифікації даних. Електронний цифровий підпис/ С.П. Чігірьов, С.І. Ганжела // Збірник тез доповідей Всеукраїнського студентського науково-практичного семінару "Сучасні інформаційні технології та програмне забезпечення комп’ютерних систем". – Кіровоград: Вид-во "КОД", 2012. – С. 45-47.

13. Інформаційні ресурси

1. Стандарт ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення» http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=120158&cat_id=119123.