МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Східноєвропейський національний університет
імені Лесі Українки

Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
Криптографічний та стеганографічний захист інформації

Освітній рівень: бакалавр
Галузь знань: 12 Інформаційні технології
Спеціальність: 125 Кібербезпека

Затверджено на засіданні кафедри
комп'ютерних наук та кібербезпеки
протокол № 3 від 05.10.2020р.

Зав. кафедри Сачук Юрій Володимирович

Луцьк – 2020

Розробники: Головін Микола Борисович, кандидат фізико-математичних наук, доцент кафедри комп'ютерних наук та кібербезпеки
Сачук Юрій Володимирович кандидат фізико-математичних наук, старший викладач кафедри комп'ютерних наук та кібербезпеки.

1. Опис навчальної дисципліни

Характеристика навчальної дисципліни подається згідно з навчальним планом і представляється у вигляді таблиці 1.

Таблиця 1

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, спеціальність, освітня програма, освітній ступінь</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Денна форма навчання</td><td rowspan="8">12 - Інформаційні технології
125 - Кібербезпека

Бакалавр</td><td>нормативна</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 135/4,5</td><td>Рік підготовки третій</td></tr>
<tr><td>Семестр 5</td></tr>
<tr><td rowspan="4">ІНДЗ: є</td><td>Лекції 36 год.</td></tr>
<tr><td>Практичні 0 год.
Лабораторні 36 год.</td></tr>
<tr><td>Самостійна робота 56 год.
Консультації 7 год.</td></tr>
<tr><td>Форма контролю: екзамен</td></tr>
</table>

2. Анотація курсу

Силабус навчальної дисципліни «Криптографічний та стеганографічний захист інформації» складена відповідно до освітньо-професійної програми підготовки ОКР "Бакалавр", підготовки бакалавра галузі знань 12 - Інформаційні технології, спеціальність 125 - Кібербезпека, освітньо-професійна програма - Інформаційна безпека.

Предметом вивчення навчальної дисципліни Криптографічний та стеганографічний захист інформації є:

- криптографічні шифри;
- методи стеганографії;
- алгоритми та протоколи шифрування та приховування інформації;

Місце навчальної дисципліни в системі професійної підготовки фахівця: дисципліна «Криптографічний та стеганографічний захист інформації» належить до нормативних фундаментальних дисциплін і є базовою для вивчення спеціальних курсів студентами спеціальності 125 – Кібербезпека. Це одна із ***основних складових*** циклу ***професійної*** підготовки. Навчальна дисципліна спирається на вищу математику, теорію інформації та кодування і формує знання для засвоєння дисциплін пов'язаних з безпекою інформаційних та комунікаційних систем.

Програма навчальної дисципліни складається з наступних **змістових модулів**.

1. Фундаментальні поняття криптографії та сутність криптографічного перетворення інформації.
2. Характеристики та способи реалізації сучасних криптографічних та стеганографічних алгоритмів

Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни «Криптографічний та стеганографічний захист інформації» є ознайомлення з теоретичними основами криптографії і стеганографії та практичними напрямами їх застосування.

Основними завданнями вивчення дисципліни «Криптографічний та стеганографічний захист інформації» є:

- закладання основ знань та умінь стосовно принципів побудови, впровадження та налагодження криптографічних систем захисту інформації;
- вивчення методів стеганографічного приховування інформації.

Згідно з вимогами освітньо-професійної програми студенти повинні:

знати

- технології шифрування інформації;
- технології приховування інформації (стеганографії);
- методи криптоаналізу повідомлень;
- методи стеганографичного аналізу файлів;

вміти :

- застосовувати шифрування інформації на практиці;
- приховувати інформацію в файлах;
- застосовувати методи криптоаналізу повідомлень;
- аналізувати медіа файли на предмет приховування інформації.

На вивчення навчальної дисципліни відводиться 120 годин / 4 кредитів ECTS.

Форма контролю – екзамен.

3. Компетенції

Інтегральна компетентність (ІНТ)

Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

Загальні компетентності (ЗК)

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професії.

ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.

Фахові компетентності (ФК)

ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

Програмні результати навчання

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

4. Інформаційний обсяг навчальної дисципліни

Структура навчальної дисципліни

Структура навчальної дисципліни представляється у вигляді таблиці 2.

Таблиця 2.

Назви змістових модулів і тем	Кількість годин					
	Усього	у тому числі				
		Лек.	Практ. (Семін.)	Лаб.	Сам. роб.	Конс.
1	2	3	4	5	6	7
Модуль 1. Фундаментальні поняття криптографії та сутність криптографічного та стеганографічного перетворення інформації						
Тема 1. Цілі і завдання криптографії. Криптографічне перетворення інформації. Основні поняття. Історія захисту інформації.	8	2		2	4	
Тема 2. Основні класи симетричних криптосистем. Алгоритмічні та програмні реалізації простих симетричних шифрів.	10	2		4	4	
Тема 3. Програмні реалізації деяких традиційних симетричних криптосистем. Види сучасних симетричних шифрів.	8	2		2	4	
Тема 4. Алгоритм DES та його модифікації	8	2		2	4	
Тема 5. Характеристика потокових шифрів.	8	2		2	4	
Тема 6. Класи асиметричних криптосистем. Переваги і недоліки асиметричних шифрів в порівнянні з симетричними. Деякі реалізації.	11	4		2	4	1
Тема 7. Алгоритмічні та програмні реалізації простих асиметричних шифрів.	14	4		4	4	2
Усього годин за перший модуль	67	18		18	28	3
Модуль 2. Характеристики та способи реалізації сучасних криптографічних та стеганографічних алгоритмів						
Тема 8. Види сучасних асиметричних шифрів. Алгоритми RSA та Ель-Гамаля	7	2		2	3	
Тема 9. Криптосистеми на еліптичних кривих	7	2		2	3	
Тема 10. Криптоаналіз шифрів. Стійкість шрифтів до зламу.	7	2		2	3	
Тема 11. Стеганографічні методи захисту інформації. Основні поняття. Принципи приховування інформації.	7	2		2	3	
Тема 12. Алгоритмічні та програмні реалізації простих способів приховування інформації в графічних файлах.	10	2		4	4	
Тема 13. Алгоритмічні та програмні реалізації простих способів приховування інформації в звукових файлах.	10	4		2	4	
Тема 14. Методи текстової стеганографії.	10	2		2	4	2
Тема 15. Принципи стеганографічного аналізу	10	2		2	4	2
Усього годин за другий модуль	68	18		18	28	4
Усього годин	**135**	**36**		**36**	**56**	**7**

Теми лабораторних занять

Таблиця 3.

№ з/п	Тема	Кількість годин
1	Цілі і завдання криптографії. Криптографічне перетворення інформації. Основні поняття. Історія захисту інформації.	2 год
2	Основні класи симетричних криптосистем. Алгоритмічні та програмні реалізації простих симетричних шифрів.	4 год
3	Програмні реалізації деяких традиційних симетричних криптосистем. Види сучасних симетричних шифрів.	2 год
4	Алгоритм DES та його модифікації	2 год
5	Характеристика потокових шифрів.	2 год
6	Класи асиметричних криптосистем. Переваги і недоліки асиметричних шифрів в порівнянні з симетричними. Деякі реалізації.	2 год
7	Алгоритмічні та програмні реалізації простих асиметричних шифрів.	4 год
8	Види сучасних асиметричних шифрів. Алгоритми RSA та Ель-Гамаля	2 год
9	Криптосистеми на еліптичних кривих	2 год
10	Криптоаналіз шифрів. Стійкість шрифтів до зламу.	2год
11	Стеганографічні методи захисту інформації. Основні поняття. Принципи приховування інформації.	2 год
12	Алгоритмічні та програмні реалізації простих способів приховування інформації в графічних файлах.	4 год
13	Алгоритмічні та програмні реалізації простих способів приховування інформації в звукових файлах.	2 год
14	Методи текстової стеганографії.	2 год
15	Принципи стеганографічного аналізу	2 год
	Усього годин	36 год

5. Завдання для самостійного опрацювання

Самостійна робота студента складається з кількох частин.

1. Опрацювання лекційного матеріалу, що дублюється і розширюється матеріалами інформаційної частини відповідного дистанційного курсу на платформі MOODLE.
2. Підготовка до лабораторних занять, яка, зокрема, полягає в виконанні тестових завдань, що викладені в достатній кількості на дистанційній платформі MOODLE і підтримують кожну тему курсу.
3. Виконання індивідуальних програмних проектів для студентів, які претендують на високі оцінки. Пошук та засвоєння додаткових матеріалів необхідних для реалізації проекту. Маються на увазі матеріали, які дотичні до основного курсу, однак не розглядаються в курсі лекцій.
4. Систематизація вивченого матеріалу перед іспитом.

6. Види індивідуальних науково-дослідних завдань

Передбачається виконання індивідуальних програмних проектів. Тематика проектів безпосередньо пов’язана з курсом і стосується роботи з файлами, захисту інформації методом її шифрування та приховування.

7. Розподіл балів та критерії оцінювання

Поточний контроль (макс = 40 балів)															Модульний контроль		Загальна кількість балів
Модуль 1															Модуль 2	Модуль 3	
Змістовий модуль1							Змістовий модуль 2								ІНДЗ	МКР 1	МКР 2	
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				
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	10	30	30	100

Підсумковий контроль успішності навчання формується двома складовими: **поточним** та **модульним контролем**. Оцінювання знань здійснюється із використанням **100** бальної шкали.

Поточний контроль. Виконання пакетів завдань в кожній з **15** тем по першому і другому змістовному модулю дає по **2** бали. Всього на тестах в поточному контролі можна отримати максимально **30** балів. Інформація стосовно виконань завдань поточного контролю знаходиться в журналі відповідного MOODLE курсу. Оцінка за виконаний тест лабораторного заняття вказує на степінь **ознайомлення** студента з новим матеріалом відповідної теми. Використання інформаційної складової курсу під час виконання тестів поточного контролю допускається. Обмеження по часу виконання пакету завдань відсутнє. Можливості стосовно **застосування отриманих** знань на практиці оцінюються проектом, який виконує студент. Проект вважається індивідуальним завданням (**ІНДЗ**). За проект в поточному оцінюванні студент може отримати максимум **10** балів.

Модульний контроль складається з двох модульних контрольних робіт (**МКР**), що відповідні першому і другому змістовному модулю. Пакет завдань МКР містить завдання з відповідних тем змістовного модуля. Завдання з пакету вибираються випадковим чином. Кожна з модульних контрольних робіт може бути оцінена максимум на **30** балів. Всього за дві МКР можна набрати максимум **60** балів. Використання інформаційної складової курсу під час виконання тестів модульного контролю не допускається. Існує обмеження по часу виконання пакету завдань. Дається одна спроба на виконання кожної МКР. Інформація стосовно виконань завдань модульного контролю знаходиться в журналі відповідного MOODLE курсу. Вважається, що студенти готуючись МКР **закріплюють** новий матеріал. Після МКР студенти мають вільно володіти матеріалом і застосовувати його на практиці з мінімальним використанням довідкової інформації.

Екзамен проводиться в тестовій формі. На екзамені максимально можна набрати **60** балів. Екзамен здають студенти незадоволені своєю оцінкою за курс, а також ті, що набрали менше 75 балів. Пакет екзаменаційних завдань формується з всієї сукупності завдань курсу. Завдання з пакету вибираються випадковим чином. Час проведення екзамену обмежений. Дається одна спроба на виконання пакету екзаменаційних завдань. Використання інформаційної складової курсу на екзамені забороняється. Студент, що йде на екзамен обнуляє результати МКР.

Шкала оцінювання (національна та ECTS)

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену,	для заліку
90 – 100	A	Відмінно	Зараховано
82 – 89	B	Добре	
75 - 81	C		
67 -74	D	Задовільно	
60 - 66	E		
1 – 59	Fx	Незадовільно	Незараховано (з можливістю повторного складання)

8. Методичне забезпечення та рекомендована література

Перелік методичних видань для забезпечення вивчення навчальної дисципліни:

Дисципліна має підтримку дистанційного курсу «Криптографічний та стеганографічний захист інформації» на платформі MOODLE http://194.44.187.60/moodle/course/view.php?id=1396 . В цьому курсі крім інформаційної частини є потужна інтерактивна складова в вигляді пакетів тестових завдань, що сприяють систематизації, усвідомленню та закріпленню нового матеріалу по кожній темі. Також безпосередньо в курсі можна запускати та відлагоджувати програми online.

Література

1. Урбанович П.П.Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студентов /П.П.Урбанович. – Минск: БГТУ, 2016. – 220 с
2. Романьков В.А. Введение в криптографию. Курс лекций / В.А.Романьков. — М.: ФОРУМ, 2012. — 240 с.
3. Кузнецов О.О. Стеганографія:навчальний посібник / О.О.Кузнецов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.
4. Ожиганов А.Л. Криптография: учебное пособие. /А.Л.Ожиганов - СПб: Университет ИТМО, 2016.-140 с.
5. А.В.Аграновский, Р.А.Хади Практическая криптография: алгоритмы и их программирование / А.В.Аграновский, Р.А.Хади — М.: СОЛОН-Пресс, 2009. 256 с.
6. Венбо Мао Современная криптография: теория и практика. : Пер. с англ./ Мао Венбо— М. : Издательский дом "Вильяме", 2005. — 768 с.
7. Головін М.Б. Захист інформації стеганографічним способом мовою Python засобами графічної бібліотеки Pillow / Н.А.Головіна, С.М.Яцюк, Ю.В.Сачук // Комп'ютерно-інтегровані технології: освіта, наука, виробництво - Луцьк, 2020. Випуск № 40 с.110-115 http://cit-journal.com.ua/index.php/cit/article/view/166
8. Головін М.Б. Фур'є перетворення в якості аплікації спектрального аналізу звуків у курсах комп'ютерної фізики та захисту інформації // М.Б.Головін, Н.А.Головіна // Комп'ютерно-інтегровані технології: освіта, наука, виробництво - Луцьк, 2021. Випуск № 42. –С.37-42.
9. Вельшенбах М.Криптография на Си и С++ в действии. Учебное пособие /М.Вельшенбах — М.: Издательство Триумф, 2004 — 464 с.
10. Фергюсон Нильс, Шнайер Брюс Практическая криптография. : Пер. с англ. /Нильс Фергюсон, Брюс Шнайер — М: Издательский дом "Вильямс", 2005. — 424 с.
11. Смарт Н. Криптография /Н.Смарт – Москва: Техносфера, 2005. - 528 с.
12. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : «МК-Пресс», 2006. – 288 с.
13. Бьярне Страуструп Программирование: принципы и практика с использованием С++, 2-е изд. : Пер. с англ. - М. : ООО "И.Д. Вильяме", 2016. - 1328 с.
14. Шлее М. Qt 5.10. Профессиональное программирование на С++.— СПб.: БХВ-Петербург, 2018. — 1072 с.
15. Скотт Мейерс Эффективный и современный С++: 42 рекомендации но использованию С++11 и С++14. : Пер. с англ. - М. : ООО "ИД. Вильяме", 2016. - 304 с.
16. Гамма Э., Хелм Р., Джонсон Р., Влиссидес Дж. Приемы объектно-ориентированного проектирования. Паттерны проектирования. — СПб.: Питер, 2015. — 368 с.
17. Галовиц Я. С++17 STL Стандартная библиотека шаблонов. — СПб.: Питер. 2018. — 432 с.

Політика курсу

Політика цього курсу визначається місцем його в системі підготовки студентів. Це нормативний курс з циклу професійної підготовки. Як викладач, для забезпечення знань, умінь та навичок студентів та здобуття потрібних компетенцій, я підготував та ввів в дію дистанційний курсу «Криптографічний та стеганографічний захист інформації» на платформі MOODLE http://194.44.187.60/moodle/course/view.php?id=1396 . Інформаційна частини цього курсу повністю охоплює матеріал курсу. В цьому курсі є також потужна інтерактивна складова в вигляді пакетів тестових завдань. Кожен пакет містить кілька десятків завдань. Виконання завдань по кожній темі сприяє систематизації, усвідомленню та закріпленню нового матеріалу.

Робота зі студентами передбачена, як в традиційному режимі, коли студенти присутні на заняттях очно і працюють на лекціях, лабораторних та консультаціях, так і в повністю дистанційному режимі. Зрозуміло, що можливі і проміжні протоколи роботи з студентами, коли частина занять проводиться дистанційно, а частина очно.

Оцінювання. Протягом семестру для перевірки знань студентів та контролю за самостійною роботою студента застосовують лабораторні роботи. Вважається, що процес освоєння матеріалу має кілька градацій.

На першому етапі, назвемо його **ознайомлювально орієнтаційним,** студенту необхідно прослухати лекцію або прочитати відповідну інформаційну частину в moodle курсі і виконати тестові завдання теми. Це невелика порція матеріалу і контроль за часом виконання завдань і використанням інформаційної частини курсу не проводиться. Оцінюється ця частина роботи в 2 бали в поточному контролі. На протязі курсу в 15 темах можна набрати **30 балів**.

На другому, етапі засвоєння матеріалу студент має практично застосувати отримані знання. Назвемо його **структурно систематизаційним**. Тобто відбувається систематизація та структурування знань в контексті практичного використання нового матеріалу. Цей етап триває на протязі всього курсу в процесі реалізації власного проекту. На цьому етапі можна набрати **10 балів**. Передбачається представлення проекту та його захист. В процесі захисту студент повинен сказати коротко, по кілька речень по кожному наступному пункту, тема роботи, огляд подібних робіт, актуальність напрямку роботи, мета роботи, завдання роботи, математична модель, алгоритм реалізації задуму, вибір інструменту реалізації задуму, реалізація, обговорення ключових цікавих моментів реалізації, апробація та обговорення результатів, висновки.

Останній третій етап, назвемо його **закріплювально завершальним,** пов'язаний з остаточним закріпленням матеріалу курсу в процесі підготовки до модульних контрольних робіт або екзамену. Виконання двох контрольних модульних робіт оцінюється по **30 балів**, екзаменаційної роботи **60 балів**. Тут перевіряються великі порції матеріалу проводиться контроль за часом виконання завдань. Використанням інформаційної частини курсу заборонено. Оцінюється ця частина роботи в модульному або екзаменаційному контролі.

Відвідування. Зазначалось, що курс може бути проведений, як повністю очний, так і повністю дистанційний. Зрозуміло, що можуть бути реалізовані будь які комбіновані варіанти. Однак в повність дистанційному курсі виникає проблема доброчесності. Ніколи неможна бути до кінця впевненим, що студент сам виконує завдання і взагалі є причетним до будь-яких результатів зворотного зв’язку курсу. Тому в політиці курсу є вимога очної присутності на модульних контрольних заходах. Та вимога очного захисту власного проекту.

Щодо академічної доброчесності. Під час виконання модульної, підсумкової контрольної роботи вважається шахрайством заглядання в будь-які інформаційні ресурси розташовані в додаткових вікнах, закладках екрану, на мобільному телефоні, шпаргалках, конспекті, підручнику. Заборонено також підказувати та слухати підказки. Проект студента повинен перевірятись на плагіат і має бути захищений персонально.

Криптографічний та стеганографічний захист інформації є галуззю знань, що постійно трансформується та модифікується. Тому цей курс теж змінюється. Покращується інформаційна частина курсу, добавляються нові завдання. В процесі поточного розгляду матеріалів приймаються всілякі побажання до інформаційної частини курсу, в процесі поточного контролю передбачає обговорення тестових завдань та їх корекція. На етапі модульного контролю будь-які претензії студентів, як до інформаційної частини курсу, так і до завдань не приймаються.

Академічна доброчесність базується на згоді усіх учасників процесу навчання: викладач та студенти, дотримуватися правил та виконувати узяті зобов'язання.

9. Перелік питань до екзамену

Екзамен проводиться автоматизовано через тестову частину курсу. Пакет екзаменаційних завдань і модульних контрольних робіт формується з числа завдань, що розглядались в процесі поточного контролю. Всі ці завдання виконувались студентами. Стосовно всіх завдань приймались зауваження і побажання. Ускладнення ситуації екзамену або модульної контрольної роботи полягає в забороні користування інформаційними ресурсами, обмежені часу виконання завдань, в великій кількості цих завдань, широкому охоплені матеріалу, що контролюється та в випадковому виборі конкретних завдань.