МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
нормативного освітнього компонента

КРИПТОГРАФІЯ ТА СТЕГАНОГРАФІЯ

Підготовки	**бакалавра**
Спеціальності	**125 Кібербезпека та захист інформації**
Освітньо-професійної програми	**12 Інформаційні технології**

Луцьк – 2023

Силабус навчальної дисципліни «Криптографія та стеганографія» підготовки бакалавра, галузь знань - 12 «Інформаційні технології», спеціальності - 125 «Кібербезпека», за освітньо-професійною програмою - «Інформаційна безпека»

Розробник: Головін Микола Борисович, кандидат фізико-математичних наук, доцент кафедри комп'ютерних наук та кібербезпеки

Погоджено
Гарант освітньо-професійної програми:  Глинчук Л.Я.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 2 від 28.09.2023 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній ступінь</th><th>Характеристика освітнього компонента
денна форма навчання</th></tr>
<tr><td>Денна форма навчання</td><td rowspan="8">12 - Інформаційні технології
125 - Кібербезпека
Інформаційна безпека
Бакалавр</td><td>Нормативна</td></tr>
<tr><td>Кількість годин/кредитів 150/5</td><td>Рік підготовки другий</td></tr>
<tr><td rowspan="6">ІНДЗ: є</td><td>Семестр 4</td></tr>
<tr><td>Лекції 44 год.</td></tr>
<tr><td>Лабораторні 66 год.</td></tr>
<tr><td>Самостійна робота 30 год.</td></tr>
<tr><td>Консультації 9 год.</td></tr>
<tr><td>Форма контролю: екзамен</td></tr>
<tr><td colspan="2">Мова навчання</td><td>українська</td></tr>
</table>

ІІ. Інформація про викладача (- ів)

ПІП _____Головін Микола Борисович_____
Науковий ступінь ____кандидат фіз.-мат.наук_____
Вчене звання _____доцент_____
Посада _____доцент_____
Контактна інформація Golovin_Mykola@vnu.edu.ua
Дні занять *http://194.44.187.20/cgi-bin/timetable.cgi?n=700*

ІІІ. Опис освітнього компонента

1. Анотація курсу

Силабус навчальної дисципліни «Криптографія та стеганографія» 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 студентами спеціальності 125 – Кібербезпека. Це одна із ***основних складових*** циклу ***професійної*** підготовки. Програма навчальної дисципліни складається з наступних **змістових модулів.**

- Сутність криптографічного захисту інформації.
- Стеганографічні методи захисту інформації**.**

2. Пререквізити та постреквізити.

Пререквізити. Навчальна дисципліна спирається на вищу математику, теорію інформації та її кодування. **Постреквізити**. Навчальна дисципліна формує знання необхідні для засвоєння дисциплін пов'язаних з безпекою інформаційних та комунікаційних систем.

3. Мета та завдання освітнього компонента

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 та стеганографічнних систем захисту інформації. Згідно з вимогами освітньо-професійної програми студенти повинні:

знати

- технології шифрування та приховування інформації;
- методи криптоаналізу повідомлень;
- методи стеганографичного аналізу файлів;

вміти :

- застосовувати шифрування та приховування інформації на практиці;
- застосовувати методи криптоаналізу повідомлень;
- аналізувати медіа файли на предмет приховування інформації.

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

4. 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 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.

Фахові компетентності (ФК)

ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.
ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики

безпеки.
ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання

ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.
ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
ПРН 35. 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.
ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

5. Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам.	Конс.	Бали
Змістовий модуль 1. Концепції криптографії та шифри з закритим ключем						
Тема 1. Цілі, завдання криптографії та стеганографії. Основні поняття. Історія захисту інформації. Основні класи симетричних та асиметричних криптосистем.	6	2	2	2		С/1
Тема 2. Кодування текстової та числової інформації. ASCII. Юникод. Двійкова, вісімкова, шиснадцяткова системи числення.	9	2	4	2		Т/2
Тема 3. Шифрування зміщенням коду. Генератори випадкових і псевдовипадкових чисел. Підстановочний шифр. Книжний шифр. Одноразовий шифроблокнот.	12	4	6	2	1	Т/3
Тема 4. Перестановочний шифр. Ключ з випадкових чисел, що не повторюються. Шифрування, дешифрування.	11	4	4	2	1	Т/3
Тема 5. Алгоритмічні та програмні реалізації простих симетричних шифрів на мові Python.	13	4	6	2	1	Т/3
Тема 6. Частотный анализ. Програмні реалізацій зламу шифрів на прикладі: афінного, підстановочного, перестановочного, Виженера, Цезаря	15	4	6	4	1	Т/3
Модульна контрольна 1	2		2			Т/30
Усього годин за перший модуль	68	20	30	14	4	45
Змістовий модуль 2. Криптосистеми із відкритим ключем та стеганографія						
Тема 7. Концепції асиметричного шифрування. Програмна реалізація розрахунку обміну ключами Діффі-Хеллмана (Python)	11	4	4	2	1	Т/3
Тема 8. Алгоритми RSA та Ель-Гамаля. Реалізація алгоритму RSA для малих значень на мові. Python Програмна реалізація шифрування з відкритим ключем	13	4	6	2	1	Т/3
Тема 9. Переваги і недоліки асиметричних шифрів в порівнянні з симетричними. Криптоаналіз шифрів. Стійкість шрифтів до зламу.	11	4	4	2	1	Т/3
Тема 10. Приховування інформації. Формати медійних файлів. Стеганографічні методи захисту інформації. Основні поняття. Методи текстової стеганографії. Мережева стеганографія.	13	4	6	2	1	Т/2
Тема 11. Технологія LSB. Алгоритмічні та програмні реалізації на Python простих способів приховування інформації в графічних і звукових файлах.	15	4	6	4	1	Т/3
Тема 12. Принципи стеганографічного аналізу.	13	4	4	4	1	С/1
Модульна контрольна 2	2		2			Т/30
Захисти проектів (ІНДЗ)	4		4			П/10
Усього годин за другий модуль	82	24	36	16	6	55
Усього годин	**150**	**44**	**66**	**30**	**10**	**100**

Методи контролю*: Т-тест, С-семінар, П-захист проекту

6. 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. Виконання тестових завдань, що викладені в достатній кількості на дистанційній платформі MOODLE і підтримують кожну тему курсу. Цією роботою реалізується також і підготовка до відповідних лабораторних занять.

3. Виконання індивідуальних програмних проектів для студентів, які претендують на високі оцінки. Тематика проектів безпосередньо пов'язана з курсом і стосується захисту інформації, методів її шифрування та приховування, роботи з відповідними файлами. Пошук та засвоєння додаткових матеріалів необхідних для реалізації проектів. Маються на увазі матеріали, які дотичні до основного курсу, однак не розглядаються в курсі лекцій.

4. Проходження інших, зовнішніх відповідних тематиці дисципліни дистанційних курсів, на кшталт, курсу з пакету Coursera (https://www.coursera.org/learn/crypto#syllabus)

5. Систематизація вивченого матеріалу перед іспитом.

IV. Політика оцінювання

Політика викладача щодо здобувача освіти.

Поточний контроль успішності в цьому курсі реалізується виконанням тестів по окремим темам, що згруповані в двох змістовних модулях та викладені в Moodle курсі. Ці дві групи тестів дають по **15** балів **поточного контролю**, кожна. Всього **30** балів поточного контролю можна набрати тестами. Ще **10** балів в поточний контроль дає **ІНДЗ.**

Контрольні заходи впродовж навчання реалізуються двома модульними контрольними роботами. Кожна з цих контрольних робіт оцінюються в межах **30** балів кожна.

Це підхід відображений в відповідній таблиці розподілу балів по формам контролю нижче.

Таблиця Розподілу балів по формам контролю

Поточний контроль(макс = 40 балів)			**Модульнийконтроль**		**Загальна кількість балів**
Модуль 1		**Модуль 2**	**Модуль 3**		
Змістовий модуль1	**Змістовий модуль 2**	**ІНДЗ**	**МКР 1**	**МКР 2**	
Тематичні тести поточного контролю					
15 балів	15 балів	10	30	30	100

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

Про тести поточного контролю. Інформація стосовно виконань тестових завдань поточного контролю знаходиться в журналі 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 тематичного пакету завдань відсутнє. Припустиме дистанційне виконання тестів. Після завершення вивчення теми можливість виконання тесту припиняються. Останнє має мотивувати студенів до систематичної роботи при дистанційному навчанні.

Про ІНДЗ. Можливості стосовно **застосування отриманих** знань на практиці оцінюються по проекту, який виконує студент. Проект вважається індивідуальним завданням (**ІНДЗ**). За проект в поточному оцінюванні студент може отримати максимум **10** балів. Ці 10 балів начисляються, як за змістовне наповнення проекту, так і за його

очний захист в присутності групи. Захист передбачає: усну доповідь з використанням наочності, демонстрацію роботи програмних засобів створених впродовж виконання ІНДЗ. Бали нараховуються також за участь в дебатах по захисту проекту. Оцінюється, як запитання опонентів в дебатах, так і відповіді доповідача.

Альтернативним індивідуальним завданням (ІНДЗ), що оцінюється в 10 балів, є проходження зовнішніх відповідних тематиці дисципліни дистанційних курсів, на кшталт, курсу https://www.coursera.org/learn/crypto#syllabus або інших подібних (по домовленості з викладачем). Свідченням про завершення зовнішнього курсу є посилання в Інтернеті на відповідний сертифікат про успішне закінчення курсу.

Про 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 оцінюється 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. Тести виконуються очно. При дистанційному виконанні тесту максимальна оцінка знижується до **20** балів. Інформація стосовно виконань завдань модульного контролю знаходиться в журналі MOODLE курсу. Вважається, що студенти готуючись МКР **закріплюють** новий матеріал. Після МКР студенти мають вільно володіти матеріалом з мінімальним використанням довідкової інформації. Робота над проектами та їх захист має вивести студентів на рівень, коли вони зможуть **застосовувати отримані знання на практиці**.

Політика щодо академічної доброчесності.

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту (https://vnu.edu.ua/uk/statut-snu-imeni-lesi-ukrayinki) і Правил внутрішнього розпорядку ВНУ імені Лесі Українки (https://vnu.edu.ua/uk/public-nformation/pravilavnutrishnogo-rozporyadku-snu-imeni-lesi-ukrayinki), загальноприйнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування. Очікується, що всі студенти відвідають усі лекції і лабораторні заняття курсу.

Кожен студент повинен ознайомитися і слідувати Кодексу академічної доброчесності Волинського національного університету імені Лесі Українки (https://ra.vnu.edu.ua/naukovizahody-ta-konkursy/konferentsiyi-ta-seminary/), дотримуватись етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності.

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання студенти не користуються забороненими засобами (мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси), самостійно виконують запропоновані завдання.

Політика щодо дедлайнів та перескладання.

Можливе, як очне, так і дистанційне проходження курсу. Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона вивчають теоретичний матеріал самостійно використовуючи інформаційну складову відповідного Moodle курсу та навчальні посібники. Тематичні завдання поточного тестового контролю виконують вчасно, адже після завершення вивчення теми можливість виконувати завдання теми припиняються. Прозвітуватися про виконання завдань можна у встановлені викладачем терміни під час консультацій. Заборгованість із модуля повинна бути ліквідована студентом до початку підсумкового контролю з наступного модуля. Кінцевий термін ліквідації заборгованості з модульного контролю обмежується початком заліково-екзаменаційної сесії.

Роботи над власними проектами (**ІНДЗ**) та їх захисти творяться впродовж семестру. Захисти проектів відбуваються в присутності студентів групи і з їх участю. Останнє може бути реалізовано, як в очному, так і в дистанційному режимі. Бали з **ІНДЗ** є поточним оцінюванням. Тому захисти проводяться до сесії.

Перескладання модульних контрольних робіт заборонено. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.

V. Підсумковий контроль

Екзамен проводиться в тестовій формі в середовищі Moodle. 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. Стосовно завдань, до екзамену, приймаються зауваження і побажання. 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.

По бажанню студент може здавати екзамен по білетам традиційним способом. Питання до екзамену нижче.

VI. Шкала оцінювання

Шкала оцінювання знань (форма контролю – іспит)

Оцінка в балах	**Лінгвістична оцінка**	**Оцінка за шкалою ECTS**	
		оцінка	**пояснення**
90–100	Відмінно	A	відмінне виконання
82–89	Дуже добре	B	вище середнього рівня
75–81	Добре	C	загалом хороша робота
67–74	Задовільно	D	непогано
60–66	Достатньо	E	виконання відповідає мінімальним критеріям
1–59	Незадовільно	Fx	Необхідне перескладання

VII. Рекомендована література та інтернет-ресурси

Методичне забезпечення

Дисципліна має підтримку дистанційного курсу «Криптографічний та стеганографічний захист інформації» на платформі MOODLE URL: http://194.44.187.60/moodle/course/view.php?id=1396 . Курс рекомендований науково-методичною радою університету до використання у навчальному процесі. Протокол № 10 від 21.06.2022. 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.

Основна література

1. Конахович Г.Ф., Прогонов Д.О., Пузиренко О.Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних [підручник]. — К. : «Центр навчальної літератури», 2018. — 558 с.
2. Al Sweigart Cracking codes with Python: an introduction to building and breaking ciphers Description: San Francisco : No Starch Press,Inc., [2018] https://elhacker.info/manuales/Lenguajes%20de%20Programacion/Python/Cracking%20Codes%20with%20Python.pdf
3. Дурняк Б.В., Музика Д.В., Сабат В.І. Стеганографічні методи захисту документів — Львів : Укр. акад. друкарства, 2014. — 159 с.
4. Урбанович П.П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студентов. – Минск: БГТУ,2016. – 220 с.
5. Кузнецов О.О., С.П. Євсеєв, О.Г. Король. Стеганографія: навчальний посібник – Х. : Вид. ХНЕУ, 2011. – 232 с.
6. Венбо Мао Современная криптография: теория и практика. : Пер. с англ.— М. : Издательский дом "Вильяме", 2005. — 768 с.
7. Блінцов В.С., Гальчевський Ю.Л. Математичні основи криптології + CD : Навчальний посібник для студ. вищих навч. закл. Національний ун-т кораблебудування ім. адмірала Макарова. - Миколаїв : НУК, 2006. - 232с.
8. Горбенко І.Д., Гріненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах : Навч. посіб. для студ. Ч. 1. Криптографічний захист інформації. Харк. нац. ун-т радіоелектрон. - Х., 2004. - 368 с.
9. Задірака В.К., Олексюк О.С. Комп'ютерна криптологія : Підручник. - Тернопільська академія народного господарства; НАН України; Інститут кібернетики ім. В.М.Глушкова. - К., 2002. - 504с.
10. Блінцов В.С., Гальчевський Ю.Л. Математичні основи криптології + CD : Навч. посіб. для студ. вищ. навч. закл. Нац. ун-т кораблебудування ім.Адмірала Макарова. - Миколаїв, 2006. - 232 с.
11. Маракова І.І., Рибак А.І., Ямпольський Ю.С. Захист інформації. Криптографічні методи : Підруч. для вищ. навч. закл. - Одес. держ. Політехн. ун-т, Ін-т радіоелектрон. і телекомунікацій. - О., 2001. - 174 с.
12. Антонов В.М., Пермяков О.Ю. Комп'ютерні мережі військового призначення . - К.: "МК-Прес", 2005. - 320 с.
13. Гарбарчук В., Зинович З., Свиц А. Кибернетический подход к проектированию систем защиты информации. Украинская академия информатики; Волынский гос. ун-т им. Леси Украинки ; Люблинский политехнический ун-т. - К. ; Луцк ; Люблин, 2003. - 658с.
14. Кузнецов О.О., Євсеєв С.П., Король О.Г. Стеганографія:навчальний посібник . – Х. : Вид. ХНЕУ, 2011. – 232 с.

15. Головін М.Б., Головіна Н.А., Яцюк С.М., Сачук Ю.В. Захист інформації стеганографічним способом мовою Python засобами графічної бібліотеки Pillow. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. Луцьк, 2020. Випуск № 40 с.110-115. URI: https://evnuir.vnu.edu.ua/handle/123456789/19701
16. Головін М.Б., Головіна Н.А. Навчальний приклад маскування інформації в акустичному сигналі. Наукові записки Бердянського державного педагогічного університету. Серія: Педагогічні науки. Бердянськ, 2021. Випуск 2. С. 203-210. URI: https://evnuir.vnu.edu.ua/handle/123456789/20108
17. Mykola Holovin, Nina Holovina Educational example of masking textual information in a photographic signal. Journal «ScienceRise: Pedagogical Education» No4(49)2022 pp24-28 URL: http://journals.uran.ua/sr_edu/article/view/261051/258566
18. Головін М.Б., Головіна Н.А. Фур'є перетворення в якості аплікації спектрального аналізу звуків у курсах комп'ютерної фізики та захисту інформації. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. Луцьк, 2021. Випуск № 42. С.37-42. URI: https://evnuir.vnu.edu.ua/handle/123456789/19750

Додаткова література

19. Фергюсон Нильс, Шнайер Брюс Практическая криптография. : Пер. с англ. — М: Издательский дом "Вильямс", 2005. — 424 с.
20. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика – К. : «МК-Пресс», 2006. – 288 с.
21. Бэрри Пол Изучаем программирование на Python [пер. с англ. М.А. Райтман]. — Москва: Издательство «Э», 2017.— 624 с.
22. Документація Python 3.8.12. URL: https://docs.python.org/3.8/index.html

7. Перелік питань до екзамену

- Цілі, завдання криптографії та стеганографії. Основні поняття. Історія захисту інформації.
- Основні класи симетричних криптосистем. Кодування та шифрування інформації. Алгоритмічні та програмні реалізації простих симетричних шифрів на мові Python.
- Класи асиметричних криптосистем. Переваги і недоліки асиметричних шифрів в порівнянні з симетричними.
- Концепції асиметричного шифрування. Протокол Ди́ффи — Хе́ллмана Програмна реалізація розрахунку ключів по алгоритму обміну ключами Діффі-Хеллмана (на мові Python).
- Види сучасних асиметричних шифрів. Алгоритми RSA та Ель-Гамаля. Реалізація алгоритму RSA для малих значень на мові Python.
- Криптоаналіз шифрів. Стійкість шрифтів до зламу.
- Стеганографічні методи захисту інформації. Основні поняття. Принципи приховування інформації.
- Алгоритмічні та програмні реалізації на мові Python простих способів приховування інформації в графічних файлах. Технологія LSB - наменший значимий біт.
- Алгоритмічні та програмні реалізації простих способів приховування інформації в звукових файлах.
- Методи текстової стеганографії.
- Мережева стеганографія.
- Принципи стеганографічного аналізу.