**КРИПТОАНАЛІЗ**

**(СИЛАБУС)**

**Викладач:** к. ф.-м. н., доцент Сергій Анатолійович Левчук

**Кафедра:** прикладної математики і механіки, 1-й корп. ЗНУ, ауд. 21-в (1й поверх)

**Email:** levchukser65@gmail.com

**Телефон:** 228-76-28 (кафедра), 289-41-11 (деканат)

|  |  |
| --- | --- |
| **Освітня програма, рівень вищої освіти** | Прикладна математика; бакалавр |
| **Статус дисципліни** | Вибіркова  |
| **Кредити ECTS** | 4 | **Навч. рік** | 2020-2021  | **Рік навчання -** 3 | **Тижні** | 12 |
| **Кількість годин** | 120 | **Кількість змістових модулів[[1]](#footnote-2)** | 6 | **Лекційні заняття –** 26 год.**Практичні заняття –** 26 год.**Самостійна робота –** 68 год. |
| **Вид контролю** | Іспит |  |
| **Посилання на курс в Moodle** | https://moodle.znu.edu.ua/course/view.php?id=11423 |
| **Консультації:** | щоп’ятниці, 16.05-17.25  |

**ОПИС КУРСУ**

**Мета курсу:** засвоєння студентами основних теоретичних відомостей, практичних вмінь та навичок по курсу «Криптоаналіз». Математична освіта сприяє формуванню абстрактного способу мислення, вмінню системно аналізувати досліджувані явища.

**ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ**

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

*-* вести дослідницьку діяльність, включаючи аналіз проблем, вибір способу і методів дослідження, а також оцінку якості результатів;

*-* використовувати і адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень і теорем;

*-* математично формалізувати постановку завдання;

*-* обирати та застосовувати математичні методи для розв’язання практичних задач дослідження, моделювання, аналізу, проектування, керування, прогнозування, прийняття рішень;

*-* використовувати сучасні технології проектування в розробці алгоритмічного та програмного забезпечення.

**ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ**

1. Гэри М., Джонсон Д. Вычислительные машины и трудно решаемые задачи. М.: Мир, 1982.
2. Теория и практика обеспечения информационной безопасности. Под редакцией П. Д. Зегжды. М.: Издательство Агентства Яхтсмен, 1996. 192 с.

**КОНТРОЛЬНІ ЗАХОДИ**

***Поточні контрольні заходи (max 60 балів):***

Поточний контроль передбачає такі ***теоретичні*** завдання:

* теоретична частина захищається студентом шляхом бесіди з викладачем за усіма восьмома лабораторними роботами, що передбачені робочою програмою.

Поточний контроль передбачає такі ***практичні*** завдання:

* розв’язання типових прикладів та звірка з еталонними відповідями за усіма восьмома лабораторними роботами, що передбачені робочою програмою.

***Підсумкові контрольні заходи(max 40 балів):***

***Теоретичний і практичний підсумковий контроль*** – виконання і захист завдань із самостійної роботи.

|  |  |  |
| --- | --- | --- |
| **Контрольний захід** | **Термін виконання** | **% від загальної оцінки** |
| **Поточний контроль (max 60%)** |  |  |
| Змістовий модуль 1 | Вид теоретичного завдання: опитування | тижні 1 – 2 | 10% |
| Вид практичного завдання: розв’язання типових прикладів та звірка з еталонними відповідями за усіма темами, що вивчаються |
| Змістовий модуль 2 | Вид теоретичного завдання: опитування  | тижні 3 – 4 | 10% |
| Вид практичного завдання: розв’язання типових прикладів та звірка з еталонними відповідями за усіма темами, що вивчаються |
| Змістовий модуль 3 | Вид теоретичного завдання: опитування  | тижні 5 – 6 | 10% |
| Вид практичного завдання: розв’язання типових прикладів та звірка з еталонними відповідями за усіма темами, що вивчаються |
| Змістовий модуль 4 | Вид теоретичного завдання: опитування  | тижні 7 – 8 | 10% |
| Вид практичного завдання: розв’язання типових прикладів та звірка з еталонними відповідями за усіма темами, що вивчаються |
| Змістовий модуль 5 | Вид теоретичного завдання: опитування  | тижні 9 – 10 | 10% |
| Вид практичного завдання: розв’язання типових прикладів та звірка з еталонними відповідями за усіма темами, що вивчаються |
| Змістовий модуль 6 | Вид теоретичного завдання: опитування  | тижні 11 –12 | 10% |
| Вид практичного завдання: розв’язання типових прикладів та звірка з еталонними відповідями за усіма темами, що вивчаються |
| **Підсумковий контроль (max 40%)** |  |  |
| Підсумкове теоретичне завдання: захист завдань із самостійної роботи | на заліку | 20% |
| Підсумкове практичне завдання: виконання завдань із самостійної роботи | на заліку | 20% |
| **Разом**  |  | **100%** |

**Шкала оцінювання: національна та ECTS**

|  |  |  |
| --- | --- | --- |
| За шкалоюECTS | За шкалою університету | За національною шкалою |
| Екзамен | Залік |
| A | 90 – 100 (відмінно) | 5 (відмінно) | Зараховано |
| B | 85 – 89 (дуже добре) | 4 (добре) |
| C | 75 – 84 (добре) |
| D | 70 – 74 (задовільно)  | 3 (задовільно) |
| E | 60 – 69 (достатньо) |
| FX | 35 – 59 (незадовільно – з можливістю повторного складання) | 2 (незадовільно) | Не зараховано |
| F | 1 – 34 (незадовільно – з обов’язковим повторним курсом) |

**РОЗКЛАД КУРСУ ЗА ТЕМАМИ І КОНТРОЛЬНІ ЗАВДАННЯ**

|  |  |  |  |
| --- | --- | --- | --- |
| **Тиждень****і вид заняття** | **Тема заняття** | **Контрольний захід** | **Кількість балів** |
| Змістовий модуль 1 |
| Тиждень 1Лекція 1 | Предмет криптоаналізу. Математичні основи | Опитування | 5 |
| Тиждень 1Парактичне заняття 1 | Предмет криптоаналізу. Математичні основи | Розв’язання типових прикладів за темою |
| Тиждень 2Лекція 2 | Предмет криптоаналізу. Математичні основи | Опитування | 5 |
| Тиждень 2Парактичне заняття 2 | Предмет криптоаналізу. Математичні основи | Розв’язання типових прикладів за темою |
| Змістовий модуль 2 |
| Тиждень 3Лекція 3 | Предмет криптоаналізу. Математичні основи | Опитування | 5 |
| Тиждень 3Парактичне заняття 3 | Предмет криптоаналізу. Математичні основи | Розв’язання типових прикладів за темою |
| Тиждень 4Лекція 4 | Комп’ютерне моделювання в криптоаналізі. Теоретичні відомості. Дешифровка файлів | Опитування | 5 |
| Тиждень 4Парактичне заняття 4 | Комп’ютерне моделювання в криптоаналізі. Теоретичні відомості. Дешифровка файлів | Розв’язання типових прикладів за темою |
| Змістовий модуль 3 |
| Тиждень 5Лекція 5 | Комп’ютерне моделювання в криптоаналізі. Теоретичні відомості. Дешифровка файлів | Опитування | 5 |
| Тиждень 5Парактичне заняття 5 | Комп’ютерне моделювання в криптоаналізі. Теоретичні відомості. Дешифровка файлів | Розв’язання типових прикладів за темою |
| Тиждень 6Лекція 6 | Комп’ютерне моделювання в криптоаналізі. Теоретичні відомості. Дешифровка файлів | Опитування | 5 |
| Тиждень 6Парактичне заняття 6 | Комп’ютерне моделювання в криптоаналізі. Теоретичні відомості. Дешифровка файлів | Розв’язання типових прикладів за темою |
| Змістовий модуль 4 |
| Тиждень 7Лекція 7 | Шифр стовбцової перестановки. Шифр подвійної перестановки | Опитування | 5 |
| Тиждень 7Парактичне заняття 7 | Шифр стовбцової перестановки. Шифр подвійної перестановки | Розв’язання типових прикладів за темою |
| Тиждень 8Лекція 8 | Шифр стовбцової перестановки. Шифр подвійної перестановки | Опитування | 5 |
| Тиждень 8Парактичне заняття 8 | Шифр стовбцової перестановки. Шифр подвійної перестановки | Розв’язання типових прикладів за темою |
| Змістовий модуль 5 |
| Тиждень 9Лекція 9 | Шифр стовбцової перестановки. Шифр подвійної перестановки | Опитування | 5 |
| Тиждень 9Парактичне заняття 9 | Шифр стовбцової перестановки. Шифр подвійної перестановки | Розв’язання типових прикладів за темою |
| Тиждень 10Лекція 10 | Шифр простої заміни | Опитування | 5 |
| Тиждень 10Парактичне заняття 10 | Шифр простої заміни | Розв’язання типових прикладів за темою |
| Змістовий модуль 6 |
| Тиждень 11Лекція 11 | Шифр простої заміни | Опитування | 5 |
| Тиждень 11Парактичне заняття 11 | Шифр простої заміни | Розв’язання типових прикладів за темою |
| Тиждень 12Лекція 12 | Шифр простої заміни | Опитування | 5 |
| Тиждень 12Парактичне заняття 12 | Шифр простої заміни | Розв’язання типових прикладів за темою |

**ОСНОВНІ ДЖЕРЕЛА**

**Основна література:**

1. Анохин М. И., Варновский Н. П., Сидельников В. М., Ященко В. В.Криптография в банковском деле. М.: МИФИ, 1997.
2. Гэри М., Джонсон Д. Вычислительные машины и трудно решаемые задачи. М.: Мир, 1982.
3. Теория и практика обеспечения информационной безопасности. Под редакцией П. Д. Зегжды. М.: Издательство Агентства Яхтсмен, 1996. 192 с.

**Додаткова література:**

1. Д. Кнут. Искусство программирования для ЭВМ. Т. 2, М.: Мир, 1977.
2. Р. Сайка. 56-разрядный код DES .расколот. на персональном компьютере. Computerworld Россия, 29 июля 1997.

**РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ[[2]](#footnote-3)**

**Відвідування занять. Регуляція пропусків.**

*Відвідування усіх занять є обов’язковим. У який спосіб і у які терміни здійснюється відпрацювання пропущених занять?*

**Політика академічної доброчесності**

*Які заходи перевірки на плагіат будуть вжиті викладачем? Які санкції будуть застосовані до студентів, що вдалися до списування, плагіату чи інших проявів недоброчесної поведінки? Надати посилання на приклади оформлення цитувань, посилань на авторів фото, ілюстрацій тощо.*

**Використання комп’ютерів/телефонів на занятті**

*Чи можна під час занять користуватися мобільними телефонами, ноутбуками, планшетами та іншими персональними гаджетами? Якщо так, за яких умов?*

**Комунікація**

*У який спосіб здійснюватиметься комунікація викладача зі студентами (електронна пошта, Moodle, інші засоби комунікації)? У який термін викладач відповідатиме на письмові запити студентів? Чи існують формальні вимоги до оформлення таких запитів? Якщо так, то які?*

***ДОДАТОК ДО СИЛАБУСУ ЗНУ – 2020-2021 рр.***

***ГРАФІК НАВЧАЛЬНОГО ПРОЦЕСУ 2020-2021 н. р.*** *(посилання на сторінку сайту ЗНУ)*

***АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ.*** Студенти і викладачі Запорізького національного університету несуть персональну відповідальність за дотримання принципів академічної доброчесності, затверджених ***Кодексом академічної доброчесності ЗНУ*:** <https://tinyurl.com/ya6yk4ad>. *Декларація академічної доброчесності здобувача вищої освіти* (додається в обов’язковому порядку до письмових кваліфікаційних робіт, виконаних здобувачем, та засвідчується особистим підписом): <https://tinyurl.com/y6wzzlu3>.

***НАВЧАЛЬНИЙ ПРОЦЕС ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТИ.*** Перевірка набутих студентами знань, навичок та вмінь (атестації, заліки, іспити та інші форми контролю) є невід’ємною складовою системи забезпечення якості освіти і проводиться відповідно до *Положення про організацію та методику проведення поточного та підсумкового семестрового контролю навчання студентів ЗНУ*: <https://tinyurl.com/y9tve4lk>**.**

***ПОВТОРНЕ ВИВЧЕННЯ ДИСЦИПЛІН, ВІДРАХУВАННЯ.*** Наявність академічної заборгованості до 6 навчальних дисциплін (в тому числі проходження практики чи виконання курсової роботи) за результатами однієї екзаменаційної сесії є підставою для надання студенту права на повторне вивчення зазначених навчальних дисциплін. Порядок повторного вивчення визначається *Положенням про порядок повторного вивчення навчальних дисциплін та повторного навчання у ЗНУ*: <https://tinyurl.com/y9pkmmp5>. Підстави та процедури відрахування студентів, у тому числі за невиконання навчального плану, регламентуються *Положенням про порядок переведення, відрахування та поновлення студентів у ЗНУ*: <https://tinyurl.com/ycds57la>.

***НЕФОРМАЛЬНА ОСВІТА.*** Порядок зарахування результатів навчання, підтверджених сертифікатами, свідоцтвами, іншими документами, здобутими поза основним місцем навчання, регулюється *Положенням про порядок визнання результатів навчання, отриманих у неформальній освіті*: <https://tinyurl.com/y8gbt4xs>.

***ВИРІШЕННЯ КОНФЛІКТІВ.*** Порядок і процедури врегулювання конфліктів, пов’язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, регламентуються *Положенням про порядок і процедури вирішення конфліктних ситуацій у ЗНУ*: <https://tinyurl.com/ycyfws9v>. Конфліктні ситуації, що виникають у сфері стипендіального забезпечення здобувачів вищої освіти, вирішуються стипендіальними комісіями факультетів, коледжів та університету в межах їх повноважень, відповідно до: *Положення про порядок призначення і виплати академічних стипендій у ЗНУ*: <https://tinyurl.com/yd6bq6p9>; *Положення про призначення та виплату соціальних стипендій у ЗНУ*: <https://tinyurl.com/y9r5dpwh>.

***ПСИХОЛОГІЧНА ДОПОМОГА.*** Телефон довіри практичного психолога (061)228-15-84 (щоденно з 9 до 21).

***ЗАПОБІГАННЯ КОРУПЦІЇ.*** Уповноважена особа з питань запобігання та виявлення корупції (Воронков В. В., 1 корп., 29 каб., тел. +38 (061) 289-14-18).

***РІВНІ МОЖЛИВОСТІ ТА ІНКЛЮЗИВНЕ ОСВІТНЄ СЕРЕДОВИЩЕ.*** Центральні входи усіх навчальних корпусів ЗНУ обладнані пандусами для забезпечення доступу осіб з інвалідністю та інших маломобільних груп населення. Допомога для здійснення входу у разі потреби надається черговими охоронцями навчальних корпусів. Якщо вам потрібна спеціалізована допомога, будь-ласка, зателефонуйте (061) 228-75-11 (начальник охорони). Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення у ЗНУ: <https://tinyurl.com/ydhcsagx>.

***РЕСУРСИ ДЛЯ НАВЧАННЯ. Наукова бібліотека***: <http://library.znu.edu.ua>. Графік роботи абонементів: понеділок – п`ятниця з 08.00 до 17.00; субота з 09.00 до 15.00.

***ЕЛЕКТРОННЕ ЗАБЕЗПЕЧЕННЯ НАВЧАННЯ (MOODLE): https://moodle.znu.edu.ua***

Якщо забули пароль/логін, направте листа з темою «Забув пароль/логін» за адресами:

· для студентів ЗНУ - moodle.znu@gmail.com, Савченко Тетяна Володимирівна

· для студентів Інженерного інституту ЗНУ - alexvask54@gmail.com, Василенко Олексій Володимирович

У листі вкажіть: прізвище, ім'я, по-батькові українською мовою; шифр групи; електронну адресу.

Якщо ви вказували електронну адресу в профілі системи Moodle ЗНУ, то використовуйте посилання для відновлення паролю https://moodle.znu.edu.ua/mod/page/view.php?id=133015.

***Центр інтенсивного вивчення іноземних мов***: http://sites.znu.edu.ua/child-advance/

***Центр німецької мови, партнер Гете-інституту***: https://www.znu.edu.ua/ukr/edu/ocznu/nim

***Школа Конфуція (вивчення китайської мови)***: http://sites.znu.edu.ua/confucius

1. [↑](#footnote-ref-2)
2. *Тут зазначається все, що важливо для курсу: наприклад, умови допуску до лабораторій, реактивів тощо. Викладач сам вирішує, що треба знати студенту для успішного проходження курсу!* [↑](#footnote-ref-3)