Заклад вищої освіти
«Міжнародний науково-технічний університет
імені академіка Юрія Бугая»

Кафедра комп'ютерних наук та інженерії програмного забезпечення

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В ІС

Силабус навчальної дисципліни

на 2021/2022 навчальний рік

Реквізити навчальної дисципліни		
Рівень вищої освіти	Другий (магістерський)	
Галузь знань	12 «Інформаційні технології»	
Статус дисципліни	Вибіркова	
Форма навчання	Денна	
Обсяг дисципліни (кредити ЄКТС/загальна кількість годин)	4 кредити/120 годин	
Семестровий контроль/ контрольні заходи	Модульний контроль	
Мова викладання	Українська	
Формат навчальної дисципліни	Змішаний (blended)	
Викладач(і)		**МОСКАЛЕНКО АРТЕМ ОЛЕКСІЙОВИЧ** **Посада:** завідувач кафедри комп'ютерних наук та інженерії програмного забезпечення **Науковий ступінь:** кандидат технічних наук **Вчене звання: -** **Профайл викладача:** *посилання* **Телефон:** +380664495928 **E-mail:** a.moskalenko@istu.edu.ua
Розміщення курсу	**Код курсу Google classroom:** jsrrz4i **Посилання Meet:** https://meet.google.com/lookup/fxauunzbha	

Програма навчальної дисципліни

1. Опис навчальної дисципліни

Метою навчальної дисципліни «Криптографічні методи захисту інформації в ІС» є формування базових знань в області криптографічних методів захисту інформації, підготовка фахівців, здатних аналізувати, обирати, застосовувати криптографічні засоби захисту інформації для розв'язання різних задач професійної діяльності.

Предмет вивчення навчальної дисципліни: симетричні та асиметричні криптографічні системи, криптографічні хеш-функції та електронний цифровий підпис, сучасні протоколи автентифікації та обміну ключами, основні сучасні напрями практичного застосування криптографії.

Результати навчання за дисципліною (РН):

РН 1. Сучасні криптографічні методи та засоби захисту інформації.

РН 2. Застосування криптографічних методів та засобів захисту інформації при проектуванні, реалізації та супроводженні інформаційних систем.

РН 3. Забезпечення конфіденційності даних з використанням криптографічних методів та засобів захисту інформації.

РН 4. Забезпечення цілісності даних з використанням криптографічних методів та засобів захисту інформації.

2. Пререквізити та постреквізити

Пререквізити: базові знання з математики та в галузі інформаційних технологій.

Постреквізити: «Переддипломна практика», «Дипломне проектування».

3. Зміст навчальної дисципліни

МОДУЛЬ 1. СИМЕТРИЧНІ ТА АСИМЕТРИЧНІ КРИПТОГРАФІЧНІ СИСТЕМИ

Тема 1. Основні поняття криптографії

Тема 2. Онови симетричної криптографії

Тема 3. Криптографічні системи з відкритим ключем

МОДУЛЬ 2. ПРАКТИЧНЕ ЗАСТОСУВАННЯ КРИПТОГРАФІЇ

Тема 4. Криптографічні хеш-функції та електронний цифровий підпис

Тема 5. Керування криптографічними ключами

Тема 6. Протоколи автентифікації та обміну ключами

Тема 7. Практичне застосування криптографії

4. Навчальні матеріали та ресурси

Основні:

1. Bruce Schneier. Applied Cryptography Protocols, Algorithms and Source Code in C – Wiley, 2017.

2. Sahadeo Padhye, Rajeev A. Sahu, Vishal Saraswat. Introduction to Cryptography – Boca Raton: CRC Press, 2018. – 268 p.

3. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.

4. Прикладна криптологія : системи шифрування: підручник /О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.:іл.

5. Getting started with OpenSSL: Cryptography basics [Електронний ресурс] – Режим доступу до ресурсу: https://opensource.com/article/19/6/cryptography-basics-openssl-part-1.

6. Вербіцький О.В. Вступ до криптології. Львів: Науково-технічна література, 1998. – 249 с. ISBN 966-7148-03-3 (966-7148-23-8).

Додаткові:

1. OpenSSL Cryptography and SSL/TLS Toolkit. Manpages for 1.1.1 [Електронний ресурс] – Режим доступу до ресурсу: https://www.openssl.org/docs/man1.1.1.

2. Кібербезпека: криптографія з PYTHON : навч. посіб. / С. П. Євсеєв, О. В. Шматко, О. Г. Король ; Харківський національний економічний університет ім. С. Кузнеця. – Харків; Львів : Новий Світ-2000, 2021. – 119 с. : іл. – ISBN 978-617-7519-70-5.

3. Математичні основи криптографії: конспект лекцій / укладачі: В. А. Фільштінський, А. В. Бережний. – Суми: Сумський державний університет, 2011. – 138 с.

4. Алферов Александр Павлович, Зубов Анатолий Юрьевич, Кузьмин Алексей Сергеевич, Черемушкин Александр Васильевич. Основы криптографии : Учеб. пособие для студ. вузов, обучающихся по группе спец. в области информ. безопасности. - М.: Гелиос АРВ, 2001. - 480с.

5. Горбенко Іван Дмитрович, Гріненко Тетяна Олексіївна. Захист інформації в інформаційно-телекомунікаційних системах : Навч. посіб. для студ. спец. "Комп'ютерні науки", "Комп'ютена інженерія", "Прикладна математика", "Інформаційна безпека" вищ. навч. закл. / Харківський національний ун-т радіоелектроніки. - Х. : ХНУРЕ, 2004. - Ч. 1 : Криптографічний захист інформації. - 368с. : рис. - ISBN 966-659-081-6.

6. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків. Форт. 2013р. , 878с.

Інформаційні ресурси:

1. Робоча програма навчальної дисципліни «Криптографічні методи захисту інформації в ІС» для здобувачів вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 122 «Комп’ютерні науки» освітньої програми «Комп’ютерні науки». [Електронний ресурс].

Навчальний контент

5. Методика опанування навчальної дисципліни

№ тижня	Тема	Заняття	Результат навчання	Контрольний захід
ЗМІСТОВНИЙ МОДУЛЬ №1. СИМЕТРИЧНІ ТА АСИМЕТРИЧНІ КРИПТОГРАФІЧНІ СИСТЕМИ				
1, 2				
3	**Т №1.** Основні поняття криптографії	**Л №1.** Основні поняття криптографії	РН 1-2	МК №1
4	**Т №2.** Онови симетричної	**Л №2.** Онови симетричної криптографії	РН 2,3	МК №1

	криптографії	**ПЗ №1.** Основи роботи з інструментами OpenSSL	РН 2,3	МК №1, захист ПЗ №1
5		**Л №3.** Огляд основних міжнародних та національних стандартів симетричного шифрування даних	РН 2,3	МК №1
		ПЗ №2. Симетричне шифрування інформації з використанням бібліотеки OpenSSL	РН 2,3	МК №1, захист ПЗ №2
6	**Т №3.** Криптографічні системи з відкритим ключем	**Л №4.** Криптографічні системи з відкритим ключем	РН 2,3	МК №1
		ПЗ №3. Асиметричне шифрування інформації з використанням бібліотеки OpenSSL	РН 2,3	МК №1, захист ПЗ №3
7		**Л №5.** Огляд основних міжнародних та національних стандартів асиметричного шифрування даних	РН 2,3	МК №1
		ПЗ №4. Асиметричне шифрування інформації з використанням бібліотеки OpenSSL	РН 2,3	МК №1, захист ПЗ №4
8	**Модульний контроль №1**			
ЗМІСТОВНИЙ МОДУЛЬ №2. ПРАКТИЧНЕ ЗАСТОСУВАННЯ КРИПТОГРАФІЇ				
9	**Т №4.** Криптографічні хеш-функції та електронний цифровий підпис	**Л №6.** Криптографічні хеш-функції та електронний цифровий підпис	РН 2,4	МК №2
		ПЗ №6. Хешування даних з використанням бібліотеки OpenSSL	РН 2,4	МК №2, захист ПЗ №6
10		**Л №7.** Огляд основних міжнародних і національних стандартів хешування даних та електронного цифрового підпису	РН 2,4	МК №2
		ПЗ №7. Формування електронного цифрового підпису засобами OpenSSL	РН 2,4	МК №2, захист ПЗ №7
11	**Т №5.** Керування криптографічними ключами	**Л №8.** Керування криптографічними ключами. Сертифікати відкритих ключів	РН 1-4	МК №2
12		**ПЗ №8.** Формування сертифікатів засобами OpenSSL	РН 1-4	МК №2, захист ПЗ №8
13		**ПЗ №9.** Формування сертифікатів засобами OpenSSL	РН 1-4	МК №2, захист ПЗ №9
14	**Т №6.** Протоколи автентифікації та обміну ключами	**Л №9.** Протоколи автентифікації та обміну ключами	РН 1-4	МК №2
15	**Т №7.** Практичне застосування криптографії	**Л №10.** Практичне застосування криптографії	РН 1-4	МК №2
16	**Модульний контроль №2**			

6. Самостійна робота здобувача вищої освіти

Основними видами самостійної роботи здобувачів вищої освіти з навчальної дисципліни «Криптографічні методи захисту інформації в ІС» є: самостійне опрацювання навчального матеріалу, підготовка до аудиторних занять (практичних занять, підсумкових контролів, захисту проектних завдань), виконання проектних завдань.

Програмою навчальної дисципліни «Криптографічні методи захисту інформації в ІС» передбачено виконання двох проектних завдань у першому та другому змістовних модулях відповідно.

Проектне завдання виконується командою у складі від трьох до п’яти здобувачів. На протязі першого тижня вивчення кожного із змістовних модулів дисципліни під керівництвом викладача здійснюється розподіл здобувачів по проектним командам. Розподіл здійснюється з урахуванням побажання здобувачів вищої освіти. Далі у кожній команді відбувається розподіл ролей. На наступному етапі кожна проектна команда обирає тематику проектного завдання. Тематика проектного завдання обирається або з переліку, запропонованого викладачем, або за пропозиціями проектних команд. Для кожної проектної команди на протязі першого тижня складається Картка планування проекту. Проектні завдання виконуються командою на протязі вивчення кожного із змістовних модулів дисципліни під керівництвом викладача та із залученням, за необхідності, відповідних фахівців галузі. Завершальним етапом виконання проектного завдання є презентація та захист проекту членами команди.

Політика та контроль

7. Політика навчальної дисципліни

Організація освітнього процесу

Згідно графіку навчального процесу, за розкладом занять, який розміщено на офіційному сайті МНТУ.

Правила відвідування занять

Здобувачі вищої освіти мають відвідувати аудиторні заняття згідно з розкладом, без запізнень. Освітня діяльність та відвідування здобувачами вищої освіти занять регламентується «Положенням про організацію освітнього процесу в МНТУ» та «Правилами внутрішнього розпорядку для студентів МНТУ».

Пропущені заняття відпрацьовуються в часи самостійної підготовки та у встановлені викладачем терміни.

Відвідування лекцій, практичних занять, а також відсутність на них, не оцінюється. Проте, здобувачам рекомендується відвідувати заняття, оскільки на них викладається теоретичний матеріал та демонструються різноманітні методи розв’язування прикладних задач, розвиваються навички та вміння в області цифрової обробки сигналів та зображень.

Правила поведінки на заняттях

Норми етичної поведінки учасників академічної спільноти визначені у Кодексі академічної етики ЗВО «Міжнародний науково-технічний університет імені академіка Юрія Бугая».

Правила захисту практичних робіт

Звіти з практичних робіт, оформлені у відповідності до вимог методичних рекомендацій, повинні бути захищені не пізніше наступного практичного заняття. Звіт

з останнього практичного заняття повинен бути захищений до дня захисту індивідуального завдання.

Захист звітів з практичних робіт може проводитись: безпосередньо під час поточного практичного заняття, на наступному практичному занятті, у час, що відведений для консультацій.

Правила захисту індивідуальних завдань

Індивідуальні завдання, виконані та оформлені у відповідності до вимог методичних рекомендацій, повинні бути захищені не пізніше останнього заняття (модульного контролю) із відповідного змістовного модулю дисципліни.

Презентація та захист індивідуальних завдань, як правило, відбувається особисто, крім випадків, визначених положеннями МНТУ.

Захист індивідуальних завдань може проводитись: під час проведення практичних занять, на останньому занятті (модульному контролі) із відповідного змістовного модулю дисципліни, у час, що відведений для консультацій.

Процедура оскарження результатів контрольних заходів оцінювання

Після отримання коментарів від викладача з аргументацією щодо оцінки, здобувач вищої освіти має право в індивідуальному порядку задати всі питання, які його/її цікавлять стосовно результатів контрольних заходів оцінювання. Якщо здобувач вищої освіти категорично не погоджуються з оцінкою, він/вона мають також навести аргументи щодо своєї позиції.

Порядок подання апеляційних скарг на результати підсумкового контролю визначено у Положенні про рейтингову систему оцінювання навчальних досягнень здобувачів вищої освіти у закладі вищої освіти «Міжнародний науково-технічний університет імені академіка Юрія Бугая».

Правила призначення заохочувальних та штрафних балів

Заохочувальні бали		**Штрафні бали**	
Критерій	**Бал**	**Критерій**	**Бал**
Участь у міжнародних, всеукраїнських або інших заходах (конкурсах) за тематикою навчальної дисципліни	3 бали	Порушення термінів виконання та захисту звітів з практичних робіт (за кожну роботу)	-2 бали
Опитування на лекційному занятті (опитування на одному занятті)	2 бали	Порушення термінів виконання, презентації та захисту індивідуальних завдань	-4 бали
Вдосконалення навчально-матеріальної бази кафедри	≤ 5 балів		
Участь у роботі наукового гуртка кафедри за тематикою навчальної дисципліни	5 балів	Злісне невиконання мір техніки безпеки при проведенні навчальних занять (за кожний випадок)	-5 балів

Політика дедлайнів та перескладань

Усі завдання виконуються у зазначені дати та час. Здобувачі несуть відповідальність за управління своїм часом, щоб завдання та проекти могли бути подані до встановленого терміну.

Політика перескладань визначена у Положенні про рейтингову систему оцінювання навчальних досягнень здобувачів вищої освіти у ЗВО «Міжнародний науково-технічний університет імені академіка Юрія Бугая».

Загальна оцінка після перескладання (ліквідації академічної заборгованості) знижується на 10%.

Політика щодо академічної доброчесності

Обов’язкове дотримання академічної доброчесності та недопущення плагіату під час виконання завдань.

Дотримання умов «Положення про академічну доброчесність здобувачів вищої освіти та науково-педагогічних працівників ЗВО «МНТУ» та Кодексу академічної етики.

Списування під час виконання контрольних робіт та модульних тестів заборонені (у т.ч. із використанням мобільних девайсів).

Плагіат у творчих роботах та презентаціях – заборонений.

8. Види контролю та рейтингова система оцінювання результатів навчання

Рейтингова система оцінювання результатів навчання здобувачів вищої освіти здійснюється відповідно до:

– Положення про рейтингову систему оцінювання навчальних досягнень здобувачів вищої освіти у закладі вищої освіти «Міжнародний науково-технічний університет імені академіка Юрія Бугая»;

– умов і критеріїв, визначених у цьому силабусі.

Система оцінювання та вимоги

Система оцінювання навчальної дисципліни	Оцінювання упродовж кожного змістовного модуля здійснюється за 100 бальною системою (до 40 балів за поточний контроль, до 60 балів за модульний контроль).
Практичні заняття	Максимальна кількість балів за кожне практичне заняття – 7 балів. 0 балів – не виконання відповідного завдання без поважних причин. 1 бал – виконання відповідних завдань без оформлення звіту з кількома помилками. 2 бали - виконання відповідних завдань без оформлення звіту з незначною кількістю помилок. 3 бали - виконання завдання та оформлення звіту з кількома негрубими помилками. 4 бали - виконання завдання та оформлення звіту з незначною кількістю помилок. 5 балів - виконання завдання, оформлення та захист звіту з незначною кількістю грубих помилок. 6 балів - виконання завдання, оформлення та захист звіту з кількома негрубими помилками. 7 балів – виконання завдання, оформлення та захист звіту з незначною кількістю помилок. При здійсненні оцінювання враховуються наявні штрафні бали для даного заняття.
Індивідуальні завдання	Максимальна кількість балів за кожне індивідуальне завдання – 12 балів. Кожний член проектної команди оцінюється індивідуально. Складовими частинами індивідуального оцінювання проектного завдання є: ➢ 0-6 балів – презентація та захист індивідуального завдання командою; ➢ 0-6 балів – виконання індивідуального звіту, оформленого у відповідності до вимог. При здійсненні оцінювання враховуються наявні штрафні бали для даного виду діяльності.
Умови допуску до підсумкового (модульного) контролю	Виконання всіх практичних завдань за відповідним змістовним модулем. Виконання проектного завдання відповідного змістовного модулю. Наявність не менше 20 балів за поточну успішність.

Середньозважений бал за навчальну дисципліну визначається як середній арифметичний бал всіх результатів модульних контролів.

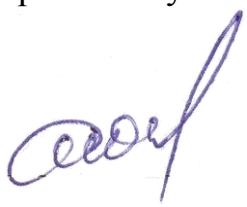
Оцінювання навчальних досягнень здобувачів вищої освіти за всіма видами контролю – здійснюється за національною системою та ECTS.

Шкала оцінювання успішності студентів

СУМА БАЛІВ	ОЦІНКА ECTS	ОЦІНКА ЗА НАЦІОНАЛЬНОЮ ШКАЛОЮ	
		екзамен	**залік**
90-100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
64-73	D	задовільно	
60-63	E		
35-59	FX	незадовільно	не зараховано
34-0	F	незадовільно	

9. Додаткова інформація з дисципліни (за потреби)

Силабус навчальної дисципліни:
складено завідувачем кафедри комп'ютерних наук та інженерії програмного забезпечення, кандидатом технічних наук Артемом МОСКАЛЕНКО



«Погоджено»
Завідувач кафедри комп'ютерних наук
та інженерії програмного забезпечення Артем МОСКАЛЕНКО