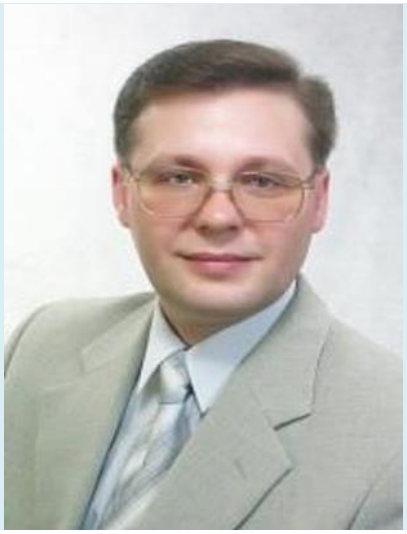
СИЛАБУС ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МЕТОДИ ПОБУДОВИ КРИПТОГРАФІЧНИХ СИСТЕМ

Факультет	Інформаційних технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	Вибіркова компонента освітніх програм другого (магістерський) рівня вищої освіти
Рекомендовано для спеціальностей	Для всіх ОПП запроваджених ДУІТЗ
Форма навчання	Денна, заочна

Викладачі

Онацький Олексій Віталійович
onatsky@meta.ua



Доцент кафедри кібербезпеки та технічного захисту інформації, кандидат технічних наук, доцент

Загальна інформація про дисципліну

Анотація до дисципліни	Дисципліна «Методи побудови криптографічних систем» рекомендована для здобувачів другого (магістерського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації. Предметом вивчення навчальної дисципліни є принципи побудови симетричних та асиметричних криптографічних систем, проблеми захисту інформації від порушення її конфіденційності, цілісності та доступності.

Мета дисципліни	формування умінь та навичок з питань захисту інформації, а саме: принципів побудови симетричних та асиметричних криптосистем, концепції криптосистем з відкритим ключем, керування криптографічними ключами, методів побудови схем електронного підпису з урахуванням сучасного стану та перспективних напрямів розвитку криптографії.
Компетентності, формуванню яких сприяє дисципліна	Здатність застосовувати знання у практичних ситуаціях. Здатність проводити дослідження на відповідному рівні. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури.
Результати навчання	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
Обсяг дисципліни	Загальний обсяг дисципліни 6 кредитів ЄКТС (180 академічних годин)
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Відповідно до розкладу занять вибіркових компонент освітньої програми

Програма дисципліни

Тема 1.	***Вимоги до реалізації сучасних криптоалгоритмів*** Параметри сучасних шифрів. Елементарні криптографічні перетворення. Побудова композиційних шифрів. Генерування блочних шифрів. Використання нелінійних структур для побудови блочних шифрів. Використання network Feistel, Modified Feistel, Substitution Permutation, unorthodox structure (own structure) для побудови блочних шифрів. Вимоги до побудови блочних криптосистем. Класифікація та призначення криптографічних перетворень.
Тема 2.	***Алгоритм шифрування DES*** Загальна характеристика DES. Схема зашифрування в алгоритмі DES. Схема обчислювання функції шифрування DES. Функційні заміни S-блоків. Схема алгоритму обчислювання ключів. Схема розшифрування в алгоритмі DES. Режими блокового шифрування: Electronic Code Book, Cipher Block Chaining. Cipher Feedback, Output Feedback, Counter Mode. Алгоритм шифрування TDEA (3DES).
Тема 3.	***Стандарт шифрування AES*** Загальна характеристика AES. Загальна схема зашифрування та розшифрування AES. Математичні основи AES. Раундові перетворення в алгоритмі AES: SubBytes, ShiftRows, MixColumns, AddRoundKey, InvShiftRows, InvSubBytes, InvMixColumns. Алгоритм розгортання ключа у стандарті AES: Key Expansion, Round Key Selection. Режими блокового шифрування AES-CTR, AES-GCM.
Тема 4.	***Алгоритм шифрування IDEA*** Загальна характеристика IDEA. Схема зашифрування в алгоритмі IDEA. Структурна схема зашифрування в алгоритмі IDEA. Генерація раундових

	ключів IDEA. Розшифрування алгоритму IDEA.
Тема 5.	***ДСТУ 7624:2014 алгоритм «Калина»*** Загальна характеристика алгоритму “Калина”. Загальна схема зашифруваннята та розшифрування алгоритму “Калина”. Математичні основи алгоритму “Калина”. Раундові перетворення в алгоритмі Калина: Add64RoundKey, SubBytes, ShiftRows, MixColumns, AddRoundKey, InvShiftRows, InvSubBytes, InvMixColumns. Схема формування циклових ключів алгоритму “Калина”. Режими роботи ДСТУ 7624:2014.
Тема 6.	***ДСТУ 8845:2019 алгоритм «Strumok»*** Принцип роботи потокового шифру. Класифікація поточних шифрів synchronous stream ciphers, asynchronous stream ciphers. Сучасні stream ciphers: A5, Salsa20, ChaCha20, Strumok. Схема функціонування генератора ключових потоків Strumok: linear feedback shift register, finite-state machine. Функція ініціалізації INIT. Функція оновлення стану NEXT. Функція ключового потоку STRM. Функція нелінійної підстановки T.
Тема 7.	***Асиметричні алгоритми шифрування*** ДСТУ 4145. ДСТУ ISO/IEC 14888-2. Протоколи на еліптичних кривих ECMQV, ECDH, ECKEP. Алгоритм електронного підпису ECDSA, ECSS, EC-GDSA, EC-KCDSA. Криптосистема NTRUEncrypt, Paillier, Optimal Asymmetrie Encryption Padding.

Список рекомендованих джерел

1. Криптографічний захист інформації: навчальний посібник з дисципліни «Криптографічний захист інформації» /О. В. Онацький, Л. Г. Йона, Ю. В. Белова; Держ. ун-т інтелект. технологій і зв’язку. – Одеса : Астропринт, 2023. – 252 с.
2. Горбенко І.Д. Прикладна криптологія. Теорія. Практика: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: Видавництво «Форт», 2012. – 880 с.
3. Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія / Ю.І. Горбенко, І.Д. Горбенко. – Харків: Видавництво «Форт», 2010. – 608 с.
4. Асиметричні методи шифрування: Навч. посіб. / Онацький О.В., Йона Л.Г., Шинкарчук Т.М.; за ред. М. В. Захарченка. – Одеса: ОНАЗ ім. О. С. Попова, 2010. – 164 с.
5. ДСТУ 4145-2002. URI: https://dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798
6. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. Мінекономрозвитку України, 2016. 228 с.
7. ДСТУ 8845-2019. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення. ДП «УкрНДНЦ», 2019. 54 с.
8. AES Rijndael Cipher explained as a Flash animation. URI: https://www.youtube.com/watch?v=gP4PqVGudtg
9. DES Animation. URI: https://www.youtube.com/watch?v=Vcld7CMAnNs
10. IDEA algorithm. URI: https://www.youtube.com/watch?v=vt1Zfs_qz3Q 11. How asymmetric (public key) encryption works. URI: https://www.youtube.com/watch?v=E5FEqGYLL0o

Інформація про консультації

Індивідуальні та колективні консультації проводяться в час, визначений за попередньою домовленістю з викладачем через засоби зв’язку.

Загальна схема оцінювання

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Шкала ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td><td rowspan="9">Нарахування балів</td><td>Бали нараховуються таким чином:</td></tr>
<tr><td>для іспиту</td><td>для заліку</td><td rowspan="8">Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою і становить: за поточну до 60 балів, за результати індивідуального завдання – до 40 балів.
При оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань здобувачів вищої освіти за різними системами</td></tr>
<tr><td>90-100</td><td>A</td><td>Відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>Незадовільно з можливістю повторного складання</td><td>Не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-34</td><td>F</td><td>Незадовільно з обов’язковим повторним вивченням дисципліни</td><td>Не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

Політика опанування дисципліни

Відвідування:
Відвідування та відпрацювання пропущених занять є обов’язковим. Допускаються пропуски занять з поважних причин, які підтверджується документально. За такої умови навчання може відбуватися в режимі он-лайн за погодженням із деканатом.
Дотримання принципів академічної доброчесності:
Політика щодо академічної доброчесності побудована на основі «Положення про академічну доброчесність» в університеті. Списування під час виконання письмових контрольних видів робіт заборонено. Користуватися мобільними пристроями, під час проведення різних видів контролю успішності, дозволяється лише з дозволу викладача.
Умови зарахування пропущених занять:
Відпрацювання пропущених занять проходять в дні згідно графіку консультацій викладачів кафедри.