СИЛАБУС ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРОГРАМУВАННЯ МЕХАНІЗМІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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

Викладачі

Кірєєв Ігор Анатолійович
kireev.igor@ukr.net

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

Загальна інформація про дисципліну

Анотація до дисципліни	Дисципліна присвячена вивченню теоретичних і практичних аспектів розробки програмних рішень для забезпечення інформаційної безпеки. Розглядаються основи програмування криптографічних алгоритмів, управління доступом, виявлення атак і захисту від них. Курс охоплює аналіз сучасних загроз, розробку засобів

	захисту та використання спеціалізованих бібліотек і інструментів.
Мета дисципліни	формування знань та навичок розробки програмного забезпечення для реалізації механізмів інформаційної безпеки, оволодіння технологіями програмування криптографічних алгоритмів, систем аутентифікації, моніторингу безпеки, а також розуміння принципів інтеграції цих механізмів у сучасні інформаційні системи.
Компетентності, формуванню яких сприяє дисципліна	Здатність застосовувати знання у практичних ситуаціях. Знання та розуміння предметної області та розуміння професії. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.
Результати навчання	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
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.	***Вступ до програмування механізмів інформаційної безпеки*** Основи інформаційної безпеки, цілі, завдання. Огляд інструментів та мов програмування для створення засобів захисту.
Тема 2.	***Основи криптографії в програмуванні*** Реалізація симетричних та асиметричних алгоритмів шифрування: AES, DES, RSA. Генерація ключів. Основи хешування (SHA, MD5).
Тема 3.	***Основи кодування та роботи з даними*** Базові принципи кодування даних: ASCII, Unicode, Base64. Перетворення тексту в закодований формат і навпаки.
Тема 4.	***Контроль цілісності даних*** Реалізація алгоритмів контрольної суми (CRC). Застосування для перевірки цілісності даних.
Тема 5.	***Основи програмування на асемблері*** Робота з регістрами, команди для маніпуляції даними, побітове кодування та декодування.
Тема 6.	***Стиснення та збереження даних***

	Програмування алгоритмів RLE (Run-Length Encoding) та Хаффмана. Побітова робота з файлами, створення власних форматів даних.
Тема 7.	***Шифрування в файлах та захист повідомлень*** Шифрування та дешифрування текстових файлів, створення захищених повідомлень за допомогою алгоритмів шифрування, зокрема шифрів на основі ключових слів.
Тема 8.	***Методи перевірки достовірності інформації*** Реалізація алгоритмів верифікації контенту (перевірка текстів, зображень, відео), використання цифрових підписів для підтвердження автентичності даних.

Список рекомендованих джерел

1. Stallings, W. (2020). Cryptography and Network Security: Principles and Practice. Pearson.
2. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.
3. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
4. Shon Harris, F., & Maymi, F. (2021). CISSP All-in-One Exam Guide. McGraw Hill.
5. Niemietz, S. (2022). Web Application Security: Exploitation and Countermeasures for Modern Web Applications. Wiley.

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="2">Нарахування балів</td><td>Бали нараховуються таким чином:</td></tr>
<tr><td>для іспиту</td><td>для заліку</td><td rowspan="6">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>
</table>

0-34	F	Незадовільно з обов’язковим повторним вивченням дисципліни	Не зараховано з обов’язковим повторним вивченням дисципліни		

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.