СИЛАБУС ОСВІТНЬОЇ КОМПОНЕНТИ

КІБЕРБЕЗПЕКА В КОМП`ЮТЕРНИХ СИСТЕМАХ

спеціальність	**не обмежено**	**обов'язковість дисципліни**	**вибіркова**
освітня програма	**не обмежено**	**факультет**	**Енергетики, робототехніки та комп'ютерних технологій**
освітній рівень	**не обмежено**	**кафедра**	**Автоматизації та комп'ютерно-інтегрованих технологій**

ВИКЛАДАЧ

Піскачова Ірина Вікторівна

Вища освіта – спеціальність електропривод та автоматизація промислових установок
Науковий ступень - кандидат технічних наук зі спеціальності озброєння і військова техніка
Вчене звання – старший науковий співробітник зі спеціальності озброєння і військова техніка
Досвід роботи – більше 12 років
Показники професійної активності з тематики курсу:

- авторка більше 100 публікацій науково-методичного характеру;
- співавторка 8 закордонних публікацій з кібербезпеки;
- учасниця міжнародного наукового проекту: Secure and resilient computing for industry and human domains. Techniques, tools and assurance cases for security and resilient computing;
- членкиня громадської організації «Українське науково-освітнє ІТ товариство;
- учасниця закордонних, міжнародних наукових конференцій з кібербезпеки.

телефон	**0509047999**	**електронна пошта**	**piskachova@btu.kharkov.ua**	**дистанційна підтримка**	**Moodle**

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ОСВІТНЮ КОМПОНЕНТУ (ДИСЦИПЛІНУ)

Мета	**підготовка студентів до використання сучасних інформаційних технологій у галузі кібербезпеки та захисту інформації, забезпечення цілісності даних, конфіденційності, контролю передачі інформації, криптографії, застосування політики безпеки**
Формат	**лекції, практичні заняття, самостійна робота**
Деталізація результатів навчання і форм їх контролю	**- формуванні у майбутніх фахівців сучасного рівня культури з інформаційної безпеки та захисту інформації;** **- набуття практичних навичок з основ застосування сучасних методів забезпечення захисту інформації в комп'ютерних системах, починаючи з криптографічних методів захисту інформації;** **- формуванні у студентів розуміння основ інформаційної безпеки, вмінню застосовувати криптографічні методи шифрування;** **- формуванні навичок використання паролів захищених систем, управління доступом різними методами; ознайомлення студентів з актуальними питаннями впливу комп'ютерних вірусів і шкідливих програм на безпеку комп'ютерних систем та методам протидії цьому, захисту мережевої інформації, у тому числі у комунікаційній сфері.**
Обсяг і форми контролю	**3 кредити ECTS (90 годин): 14 годин лекції, 30 годин лабораторно-практичні; модульний контроль (2 модулі);підсумковий контроль – диференційований залік.**
Вимоги викладача	**вчасне виконання завдань, активність, командна робота**
Умови зарахування	**вільне зарахування**

СТРУКТУРА ОСВІТНЬОЇ КОМПОНЕНТИ (ДИСЦИПЛІНИ)

Модуль 1. ТЕОРЕТИЧНІ АСПЕКТИ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ АПАРАТНИХ ТА ПРОГРАМНИХ ЗАСОБІВ.

Лекція 1.	**Вступ до дисципліни. Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення. Визначення термінів. Загальні стандарти.**	**Лабораторно-практичне заняття 1 (ЛПЗ 1, 2)**	**Системи числення** **Антивірусні програми**	**Самостійна робота**	1. **Основи захисту інформації в комп'ютерних системах** 2. **Симетричні криптологічні системи** 3. **Алгоритми симетричного шифрування** 4. **Криптосистеми із відкритим ключем** 5. **Автентіфікация та цифровий підпис** 6. **Антивірусний захист**
Лекція 2.	**Особливості забезпечення кібербезпеки апаратних комплексів. Історія розвитку та еволюція. Історія розвитку сучасних апаратних засобів для забезпечення кібербезпеки. Програмні та апаратні засоби захисту від кібератак. Загальна характеристика.**	**ЛПЗ 3,4**	**Шифрування та дешифрування шифром Цезаря** **Шифрування текстів. Основні принципи. Метод Гронсфельда. Шифри складної заміни**		

	Відмінності. Особливості застосування.				
Лекція 3.	**Апаратні та програмні засоби як об'єкт та інструмент проведення кібератак. Класифікація апаратних засобів з точку зору забезпечення кібербезпеки. Апаратні комплекси як об'єкт кібератак. Програмні та апаратні платформи для здійснення кібератак.**	**ЛПЗ 5,6**	**Алфавітний підхід до визначення кількості інформації** **Шифрування та дешифрування методом Цезаря (програмування)**		
Лекція 4.	**Сучасні вимоги та стандарти для забезпечення кібербезпеки апаратних комплексів. Сучасні стандарти забезпечення кібербезпеки.**	**ЛПЗ 7,8**	**Шифри Віжинера і Бофора** **Дослідження шифру "Подвійний квадрат"**		
Лекція 5.	**Аналіз ризиків та загроз в галузі забезпечення кібербезпеки апаратних та програмних засобів. Характеристика системи та ідентифікація загроз. Аналіз ризиків та загроз. Розрахунок ризиків та можливих впливів. Управління ризиками. Сучасні стандарти.**	**ЛПЗ 9**	**Дослідження шифру " Play Fair".**		
Лекція 6.	**Види та характеристика атак на електроні та програмні компоненти. Таксономія та класифікація видів атак на електроні компоненти. Рівні атак, їх виявлення та аналіз післядії. Інвазивні, напівінвазивні та неінвазивні атаки. Особливості застосування. Класифікація програмних компонентів та види атак. Атаки на електроні компоненти, в яких алгоритми виконуються програмно (мікроконтролери, мікропроцесори тощо).**	**ЛПЗ 10**	**Системи з закритим ключем.**		

Модуль 2. ПРАКТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ АПАРАТНИХ ТА ПРОГРАМНИХ ЗАСОБІВ.					
Лекція 7.	**Інвазивні, напівінвазивні та неінвазивні атаки на електронні компоненти. Загальна характеристика та особливості застосування. Відмінності, методи виявлення та протидії. Неінвазивні атаки - атаки сторонніми каналами. Напівінвазивні атаки - атаки на основі помилок обчислень. Інвазивні атаки - атаки засновані на фізичному втручанні.**	**ЛПЗ 11**	**Реалізація алгоритму Віженера. Макрос**		
Лекція 8.	**Атака сторонніми каналами. Класифікація видів атак. Пасивні та активні атаки. Атаки за рівнем доступу. Методи впливу та протидії. Атаки зондуванням. Атаки по енергоспоживанню. Атаки по електромагнітному випромінюванню. Акустичні атаки. Атаки по видимому випромінюванню.**	**ЛПЗ 12**	**Захист окремих листів, книги повністю і файла Excel**		
Лекція 9.	**Апаратні закладки (Trojans). Загальна характеристика. Класифікація видів та рівнів внесення апаратних закладок. Класифікація по фізичному принципу роботи. Класифікація по методу активації. Класифікація по дії на систему. Оцінка потенційної загрози. Методи виявлення.**	**ЛПЗ 13**	**Шифрування методом вертикальної перестановки с відкритим ключом**		
Лекція 10	**Захист апаратних та програмних компонентів від несанкціонованого доступу та копіювання.**	**ЛПЗ 14**	**Симетричні алгоритми шифрування DES.**		
Лекція 11	**Рівні та проблеми несанкціонованого доступу. Засоби обмеження фізичного доступу до апаратних компонентів на різних рівнях. Захист від читання. Захист**	**ЛПЗ 15**	**Асиметричні алгоритми шифрування RSA**		

	процесу завантаження та ініціалізації. Шифрування даних, що зберігаються.				

ОСНОВНА ЛІТЕРАТУРА ТА МЕТОДИЧНІ МАТЕРІАЛИ

Література

1. Домарєв В. В., Швець В. А., Шестакова В. В. Організаційне забезпечення захисту інформації з обмеженим доступом: навч. посібник. Київ: Національний авіаційний університет, 2006. 108 с.
2. Домарєв В. В., Швець В. А., Шестакова В. В. Організаційне забезпечення захисту інформації з обмеженим доступом: навч. посібник. Київ: Національний авіаційний університет, 2006. 108 с.
3. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем: підр. Київ: ДУІКТ, 2010. 316 с.

Методичне забезпечення

1. Державна служба спеціального зв'язку та захисту інформації України [Электрон. ресурс]: Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/index
2. Міжнародна організація зі стандартизації [Электрон. ресурс]. Режим доступу: https://www.iso.org/isoiec-27001-information-security.html
3. Публікації з кібербезпеки National Institute of Standards and Technologies [Електрон. ресурс]: Режим доступу: http://csrc.nist.gov/publications/PubsSPs.html #SP 800/.

Примечание [ИП1]:

СИСТЕМА ОЦІНЮВАННЯ (електронне посилання на положення)

СИСТЕМА		БАЛИ	ДІЯЛЬНІСТЬ, ЩО ОЦІНЮЄТЬСЯ
Підсумкове оцінювання	100 бальна ECTS (стандартна)	до 50	50% від усередненої оцінки за модулі
		до 50	підсумкове тестування
Модульне оцінювання	100 бальна сумарна	до 50	відповіді на тестові питання
		до 20	усні відповіді на лабораторно-практичних заняттях
		до 30	результат засвоєння блоку самостійної роботи

НОРМИ АКАДЕМІЧНОЇ ЕТИКИ ТА ДОБРОЧЕСНОСТІ

Всі учасники освітнього процесу (в тому числі здобувачі освіти) повинні дотримуватися кодексу академічної доброчесності та вимог, які прописані у положенні «Про академічну доброчесність учасників освітнього процесу ДБТУ»: виявляти дисциплінованість, вихованість, поважати гідність один одного, проявляти доброзичливість, чесність, відповідальність.