СИЛАБУС ОСВІТНЬОЇ КОМПОНЕНТИ

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

спеціальність	**не обмежено**	**обов'язковість дисципліни**	**вибіркова**
освітня програма	**не обмежено**	**факультет**	**навчально-науковий інститут «Кіберпорт»**
освітній рівень	**не обмежено**	**кафедра**	**кібернетики та інформаційних технологій**

ВИКЛАДАЧ

ЧАЛИЙ ІГОР ВІЛЬОВИЧ

Вища освіта – спеціальність „Динаміка та міцність машин"
Науковий ступень - кандидат технічних наук 05.20.01
Вчене звання - доцент кафедри кібернетики та інформаційних технологій
Досвід роботи – більше 40 років
Показники професійної активності з тематики курсу:

- автор більше 10 методичних розробок;
- співавтор 2 навчальних посібників;
- співавтор 3 тематичних публікацій (1 Scopus);
- учасник наукових і методичних конференцій.

телефон	**0503032421**	**електронна пошта**	**ivchaly@gmail.com**	**дистанційна підтримка**	**Moodle**

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ОСВІТНЮ КОМПОНЕНТУ (ДИСЦИПЛІНУ)

Мета	**ознайомлення студентів з основними поняттями інформаційної безпеки та прийомами захисту інформації, набуття компетенцій ефективно реалізовувати знання у своїй практичній та професійній діяльності.**
Формат	**лекції, практичні заняття, самостійна робота, індивідуальні завдання**
Деталізація результатів навчання і форм їх контролю	• **ознайомлення з поняттями інформаційної безпеки, як з однією із суттєвих складових частин національної безпеки країни/ лекції, практичні завдання;** • **пошук та опрацювання нормативно-правових документів щодо забезпечення інформаційної безпеки / лекції, практичні завдання;** • **засвоєння необхідних знань щодо забезпечення інформаційної безпеки та кібербезпеки, класифікації загроз інформації в комп'ютерній системі / лекції, практичні завдання, індивідуальні завдання;** • **загальна характеристика основних складових управління доступом / індивідуальні, практичні завдання, самостійна робота;** • **базові відомості про шкідливе програмне забезпечення., огляд найпоширеніших антивірусних програм / лекції, практичні завдання;** • **ознайомлення з основними принципами формування політики безпеки / індивідуальні, практичні завдання, самостійна робота** • **огляд інших засобів та методів захисту інформації, безпека бездротових та хмарних технологій / лекції, практичні завдання**
Обсяг і форми контролю	**3 кредити ECTS (90 годин): 12 годин лекції, 18 годин лабораторно-практичні; модульний контроль (2 модулі);підсумковий контроль – диференційований залік.**
Вимоги викладача	**вчасне виконання завдань, активність, самостійна робота**
Умови зарахування	**вільне зарахування**

СТРУКТУРА ОСВІТНЬОЇ КОМПОНЕНТИ (ДИСЦИПЛІНИ)

Модуль 1. ОСНОВНІ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. КІБЕРПРОСТІР, КІБЕРБЕЗПЕКА. ЗАГРОЗИ. УПРАВЛІННЯ ДОСТУПОМ.					
Лекція 1.	**Предмет та значення дисципліни. Основні визначення, що відносяться до змісту курсу. Теоретичні та нормативно-правові засади інформаційної безпеки України.**	**Лабораторно-практичне заняття 1 (ЛПЗ 1)**	**Сучасна термінологія інформаційної безпеки.**	**Самостійна робота**	**Інформаційна безпека держави. Об'єкти і суб'єкти інформаційної безпеки. Етапи розвитку інформаційної безпеки. Загрози кібертероризму. Кібервійна. Кібербезпека в умовах розгортання четвертої промислової революції: виклики та можливості для України. Персональні дані. Об'єкти захисту. Вимоги до обробки персональних даних. Біометрична ідентифікація й аутентифікація користувача. Самостійне доопрацювання матеріалів змістовного модуля 1.**
Лекція 2.	**Види та властивості інформації як предмета захисту. Кіберпростір, кібербезпека: поняття і визначення. Нормативно-правове забезпечення інформаційної безпеки.**	**ЛПЗ 2**	**Пошук та опрацювання нормативно-правових документів щодо забезпечення інформаційної безпеки**		
Лекція 3.	**Складові забезпечення інформаційної безпеки та кібербезпеки. Класифікація загроз інформації в комп'ютерній системі.**	**ЛПЗ 3**	**Кібернетичний простір та безпечний доступ до системи WWW за допомогою веб-браузера.**		
Лекція 4.	**Огляд управління доступом. Принципи безпеки.**	**ЛПЗ 4**	**Управління паролями. Правила роботи з паролями. Засоби генерації та перевірки паролів.**		
Модуль 2. ОСНОВНІ ЗАСОБИ ТА МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ.					
Лекція 5.	**Базові схеми атак та організація каналів витоку інформації. Класифікація зловмисників.**	**ЛПЗ 5**	**Дослідження видів атак на паролі. Шифрування даних за допомогою архіваторів та відновлення паролів.**	**Самостійна робота**	**Поняття авторського права. Захист авторських прав. Поняття комп'ютерного піратства. Інформаційна безпека в соціальних мережах. Засоби резервного копіювання та відновлення даних. Пристрої відновлення даних. Захисник Windows. Брандмауэр Захисника Windows в режимі підвищеної безпеки. Програмні продукти компанії Malwarebytes Ltd для захисту інформації. Самостійне доопрацювання матеріалів змістовного модуля 2.**
Лекція 6.	**Поняття шкідливого програмного забезпечення. Основні типи та загальний огляд сучасних комп'ютерних вірусів. Огляд найпоширеніших антивірусних програм та їх класифікація**	**ЛПЗ 6**	**Настроювання центра безпеки захисника Windows 10 (11).**		
Лекція 7.	**Елементи управління системою захисту інформації. Принципи формування політики безпеки.**	**ЛПЗ 7**	**Навчання (тренінги) з питань інформаційної безпеки.**		
Лекція 8	**Огляд інших засобів та методів захисту інформації. Безпека у хмарних сервісах.**	**ЛПЗ 8**	**Кваліфікований електронний підпис, як засіб безпечної передачі даних.**		

ОСНОВНА ЛІТЕРАТУРА ТА МЕТОДИЧНІ МАТЕРІАЛИ

Література

1. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.
2. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2016. 449 с.
3. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с..
4. Лахно В.А. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М . Гладких, В.М. Домрачев, Н.М. Сивкова. – К.:ЦП «Компринт» О.В., 2021. – 4 4 4 с.
5. Лютинський В.Л., Пастухов В.І., Харченко С.О., Чалий І.В. Інформаційне забезпечення сільськогосподарського виробництва. Лабораторний практикум. Частина 1. Навчальний посібник + CD. Харків, 2009. – 368 с.

Методичне забезпечення

1. Використання on-line ресурсів Інтернет для самостійного вивчення дисциплін за фахом. Методика вивчення, порядок проходження: метод. вказ. до виконання лабораторних робіт з дисциплін «Вступ до фаху та академічна доброчесність», «Основи кібербезпеки», «Кібербезпека», «Інформаційна безпека держави» / Мегель Ю.Є., Міхнова О.В., Левкін А.В., Чалий І.В., Яковенко Д.М. - Державний біотехнологічний університет, 2023. - 50 с..
2. Основи інформаційної безпеки. ч.1. Тлумачний словник. / Мегель Ю.Є., Міхнова О.В., Левкін А.В., Чалий І.В., Яковенко Д.М. - Державний біотехнологічний університет, 2023. - 72 с.
3. Настроювання центра безпеки захисника Windows 10. (частина 1). / Мегель Ю.Є., Міхнова О.В., Левкін А.В., Чалий І.В., Яковенко Д.М. - Державний біотехнологічний університет, 2023. - 50 с.
4. Хмарні технології в кібербезпеці / Мегель Ю.Є., Міхнова О.В., Левкін А.В., Чалий І.В., Яковенко Д.М. - Державний біотехнологічний університет, 2022. - 50 с.
5. Захист інформаційних ресурсів: навчально-методичний посібник до курсу – Захист інформаційних ресурсів‖ / укл. С. О. Троян. – Умань : [б.в.], 2012. –120 с.

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.