# СИЛАБУС ОСВІТНЬОЇ КОМПОНЕНТИ

## СОЦІОТЕХНІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ

| | | | |
|---|---|---|---|
| **спеціальність** | **015 Професійна освіта (агровиробництво, переробка сільськогосподарської продукції та харчові технології)** | **обов'язковість дисципліни** | **вибіркова** |
| **освітня програма** | **015 Професійна освіта (015.37 Агровиробництво, переробка сільськогосподарської продукції та харчові технології)** | **факультет** | **навчально-науковий інститут «Кіберпорт»** |
| **освітній рівень** | **перший (бакалаврський)** | **кафедра** | **інформаційних технологій, кібернетики та захисту інформації** |

## 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 2 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** | формування розуміння деяких соціотехнічних аспектів кібербезпеки, ознайомлення студентів з основними поняттями інформаційної безпеки та прийомами захисту інформації в соціальних мережах, 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 базовими поняттями: кіберпростір, інформаційна безпека, кібербезпека, та деякими іншими / лекції, практичні завдання;<br>• ознайомлення з сучасною інфосферою та особливостями її захисту в умовах стороннього кібернетичного впливу / лекції, практичні завдання;<br>• розгляд основних кіберінцидентів у сфері високих технологій / лекції, практичні завдання;<br>• вивчення основних понять та визначень, особливостей та моніторингу соціальних мереж / лекції, практичні завдання, індивідуальні завдання;<br>• розгляд концепції та принципів соціальної інженерії, її основних понять та методів / індивідуальні, практичні завдання, самостійна робота;<br>• розгляд дезінформації, як елементу кібератак / лекції, практичні завдання;<br>• розгляд пропаганди як інструменту інформаційного впливу / індивідуальні, практичні завдання, самостійна робота;<br>• надання практичних порад щодо безпечного використання соціальних мереж / лекції, практичні завдання. |
| **Обсяг і форми контролю** | 3 кредити ECTS (90 годин): 12 годин лекції, 18 годин лабораторно-практичні;<br>підсумковий контроль – залік. |
| **Вимоги викладача** | вчасне виконання завдань, активність, самостійна робота. |
| **Умови зарахування** | згідно з навчальним планом |

## ВІДПОВІДНІСТЬ СТАНДАРТУ ОСВІТИ І ОСВІТНІЙ ПРОГРАМІ

| | | | |
|---|---|---|---|
| **Компетенції** | Інтегральна компетентність.<br>Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в професійній освіті, що передбачає застосування певних теорій і методів педагогічної науки та інших наук відповідно до спеціалізації і характеризується комплексністю та невизначеністю умов.<br>Загальні компетентності:<br>К 05. Здатність приймати обґрунтовані рішення.<br>К 06. Навички використання інформаційних і комунікаційних технологій.<br>К 07. Здатність вчитися і оволодівати сучасними знаннями.<br>Спеціальні (фахові) компетентності<br>К 17. Здатність реалізовувати навчальні стратегії, засновані на конкретних критеріях для оцінювання навчальних досягнень.<br>К 18. Здатність аналізувати ефективність проектних рішень, пов'язаних з підбором, експлуатацією, удосконаленням, модернізацією технологічного обладнання та устаткування галузі/сфери відповідно до спеціалізації. | **Програмні результати навчання** | **Програмні результати навчання**<br>ПР 07. Аналізувати та оцінювати ризики, проблеми у професійній діяльності й обирати ефективні шляхи їх вирішення.<br>ПР 09. Відшуковувати, обробляти, аналізувати та оцінювати інформацію, що стосується професійної діяльності, користуватися спеціалізованим програмним забезпеченням та сучасними засобами зберігання та обробки інформації.<br>ПР 10. Знати основи психології, педагогіки, а також фундаментальних і прикладних наук (відповідно до спеціалізації) на рівні, необхідному для досягнення інших результатів навчання, передбачених цим стандартом та освітньою програмою.<br>ПР 22. Застосовувати програмне забезпечення для e-learning і дистанційного навчання і здійснювати їх навчально –методичний супровід. |

| СТРУКТУРА ОСВІТНЬОЇ КОМПОНЕНТИ (ДИСЦИПЛІНИ) | | | | | |
|---|---|---|---|---|---|
| **Тема 1. СОЦІОТЕХНІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ. СОЦІАЛЬНІ МЕРЕЖІ.** | | | | | |
| | **тема** | **Практичне заняття** | **тема** | | |
| **Лекція 1.** | **Предмет та значення дисципліни. Поняття соціотехнічної системи та її властивостей. Основні визначення та поняття, що відносяться до змісту курсу.** | **ПЗ 1,2** | **Джерела сучасної термінології 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. Сучасна інфосфера та особливості її захисту в умовах стороннього кібернетичного впливу. Самостійне доопрацювання матеріалів змістовного модуля 1.** |
| **Лекція 2.** | **Кіберпростір та кібербезпека як основа інформаційної цивілізації. Кіберінциденти у сфері високих технологій: ознаки, проблеми та реагування. Сучасна інфосфера та особливості її захисту в умовах стороннього кібернетичного впливу** | **ПЗ 3,4** | **Пошук та опрацювання матеріалів щодо кіберінцидентів у сфері високих технологій.** | | |
| **Лекція 3.** | **Соціальні мережі: основні поняття та визначення, особливості. Моніторинг соціальних мереж — цілі та способи реалізації.** | **ПЗ 5,6** | **Дослідження та характеристика найбільш поширених соціальних мереж.** | | |
| **.** | | | **LinkedIn - соціальна мережа для пошуку і встановлення ділових контактів. Дослідження матеріалів з кібербезпеки у LinkedIn** | | |
| | | | **Вибір онлайн-ресурсів для самостійного вивчення матеріалів з кібербезпеки.** | | |
| **Тема 2. МЕТОДИ І ЗАСОБИ СОЦІАЛЬНОГО ІНЖИНІРИНГУ.** | | | | | |
| **Лекція 4.** | **Концепції та принципи соціальної інженерії. Основні поняття та визначення методів соціальної інженерії. Загальні принципи. Основні етапи моделі атаки на основі методів соціальної інженерії.** | **ПЗ 7** | **Базові інструменти просування контенту в соціальних мережах.** | **Самостійна робота** | **Базові прийоми та інструменти ведення інформаційної війни у соціальних он-лайн мережах. Прийоми захисту від інформаційних атак в он-лайн мережах. Прийоми здійснення інформаційних атак в он-лайн мережах. Інтернет-технології та соціальні он-лайн мережі в структурі гібридної війни.** |
| **Лекція 5.** | **Дезінформація як елемент кібератак. Сценарії розвитку та** | **ПЗ 8** | **Самостійне проходження з отриманням сертифікатів освітніх** | | |

| | | | | | |
|---|---|---|---|---|---|
| | **методи протидії. Канали поширення дезінформації. Типи неправдивої інформації. Види маніпуляцій. Маніпуляції з медіаданими. Пропаганда як інструмент інформаційного впливу.** | | **ресурсів порталу «Дія. Освіта»** | | **Мережеві он-лайн проекти в гібридній війні: структура та принципи функціонування.<br>Самостійне доопрацювання матеріалів змістовного модуля 2.** |
| **Лекція 6.** | **Практичні поради щодо безпечного використання соціальних мереж. Способи протидії неправдивим повідомленням. Інструменти виявлення неправдивих повідомлень.** | **ПЗ 9** | **Самостійне проходження з отриманням сертифікатів освітніх ресурсів порталу «Prometheus» Кваліфікований електронний підпис, як засіб безпечної передачі даних.** | | |

## ОСНОВНА ЛІТЕРАТУРА ТА МЕТОДИЧНІ МАТЕРІАЛИ

**Література**


1. **Бурячок В.Л. Інфомаційна та кібербезпека : соціотехнічний аспект: підручник / 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. **Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: навчальний посібник / О.В.Курбан. – Київ: ВІКНУ, 2016. - 286 с.**
6. **Інформаційно-психологічне протиборство: підручник. Видання друге перекладене, доповнене та перероблене / [В. М. Петрик, В. В. Бедь, М. М. Присяжнюк та ін.]; за заг. ред. В. В. Бедь, В. М. Петрика. — К.: ПАТ «ВІПОЛ», 2018. – 386 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. **Навчальна практика (частина 1):методичні вказівки до виконання навчальної практики для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання спеціальності 125 Кібербезпека та захист інформації / Держ. біотехнологічний ун-т; авт.-уклад.: Ю.Є. Мегель, Т.А.Бутенко, А.В. Левкін, О.Д. Міхнова, Ю.В.Синявіна, І.В. Чалий – Харків : [б.-в.], 2024 – 50с.**
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

| СИСТЕМА | | БАЛИ | ДІЯЛЬНІСТЬ, ЩО ОЦІНЮЄТЬСЯ |
|---|---|---|---|
| Підсумкове оцінювання | 100 бальна ECTS (стандартна) | до 50 | 50% від усередненої оцінки за теми |
| | | до 50 | підсумкове тестування |
| Поточне 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.**