



Національний
університет оборони
України імені Івана
Черняховського

СИЛАБУС
навчальної дисципліни
«КОНЦЕПТУАЛЬНІ ПРОБЛЕМИ
ОРГАНІЗАЦІЇ БЕЗПЕКИ
ІНФОРМАЦІЙНОГО ПРОСТОРУ
ЗБРОЙНИХ СИЛ»

Рівень вищої освіти	Третій (освітньо-науковий), PhD
Спеціальність	122 Комп'ютерні науки
Статус дисципліни	Вибірковий компонент
Мова викладання	Українська
Обсяг дисципліни	3 кредити ECTS/90 год. (Л – 6 год., ГЗ – 16 год., С – 6 год., ДЗ – 4 год., СР – 60 год.)
Курс/півріччя	2 курс: 1, 2 півріччя
Оригінальність дисципліни	Авторський курс
Ключові слова	Інформаційна безпека, кібербезпека, захист інформації, кіберпростір, інформаційна операція
 Викладач	Волошко Сергій Володимирович , кандидат технічних наук, старший науковий співробітник, старший викладач кафедри зв'язку та автоматизованих систем управління інституту забезпечення військ (сил) та інформаційних технологій Сторінка в Google Scholar: https://scholar.google.com.ua/citations?hl=ru&user=JoViziQAAAAJ Наукові та навчально-методичні праці за тематикою дисципліни: 1 навчальний посібник, 3 наукові статті Підвищення кваліфікації: “Комунікаційні та інформаційні технології” за програмою НАТО – Україна з перепідготовки військовослужбовців, 28.11.2018 – 12.02.2019. Контактні дані: тел. 066-555-65-89, e-mail: sergijvolosko@gmail.com, кафедра зв'язку та автоматизованих систем управління, ауд. 2/412
Чому дисципліна для мене є важливою/ корисною/ актуальною?	Я отримаю фундаментальні знання щодо забезпечення інформаційної безпеки та кібербезпеки у Збройних Силах України, опаную необхідні вміння і навички, зможу використовувати отримані знання у майбутній професійній діяльності

Які знання я отримаю?	<p>Знання загальних положень щодо забезпечення інформаційної безпеки та кібербезпеки у Збройних Силах України;</p> <p>Знання стану і перспектив розвитку нових способів, технологій та засобів забезпечення інформаційної безпеки та кібербезпеки;</p> <p>Знання і глибоке розуміння інформаційних процесів в органах військового управління, інформаційних системах та мережах.</p> <p>Знання особливостей забезпечення інформаційної безпеки та кібербезпеки у збройних конфліктах і в ході застосування Збройних Сил в операції об'єднаних сил (антитерористичній операції).</p>
Які вміння я розвину?	<p>Вміння розв'язувати типові професійні задачі, а також проблеми, що виникають у реальних ситуаціях науково-дослідницької та педагогічної діяльності ад'юнкта з використанням знань професійної підготовки.</p> <p>Вміння управляти забезпеченням інформаційної безпеки та кібербезпеки у Збройних Силах України під час ведення бойових дій, бою і операції, розгортання системи інформаційно-аналітичного забезпечення процесів управління військовими підрозділами, їх особливостей під час участі Збройних Сил в операції об'єднаних сил (антитерористичній операції).</p> <p>Вміння розробляти та удосконалювати методи і науково-технічні пропозиції для підвищення ефективності забезпечення військ (сил).</p>
Що мене очікує?	<p>Вивчення організації системи заходів щодо забезпечення інформаційної безпеки та кібербезпеки у Збройних Силах України, використання способів, технологій та засобів забезпечення інформаційної безпеки та кібербезпеки.</p>
Якого результату я досягну?	<p>Формування фундаментальних теоретичних знань щодо забезпечення інформаційної безпеки та кібербезпеки у Збройних Силах України, використання способів, технологій та засобів забезпечення інформаційної безпеки та кібербезпеки.</p>
Де я зможу застосувати отримані знання та вміння?	<p>Під час проведення наукових досліджень.</p> <p>Під час обговорення відповідних тем на наукових конференціях, семінарах, круглих столах, нарадах, дискусіях, суперечках тощо.</p>
Зміст навчальної дисципліни	<p>Тема 1. Основи інформаційної безпеки.</p> <p>Л 1/1. Основні положення інформаційної безпеки.</p> <p>ГЗ 1/2. Законодавчий та адміністративний рівні інформаційної безпеки.</p> <p>ГЗ 1/3. Організаційний та технічний рівні інформаційної безпеки.</p> <p>ГЗ 1/4. Програмно-технічний рівень інформаційної безпеки.</p>

	<p>Тема 2. Сутність кібербезпеки держави та основні проблеми її забезпечення. Л 2/1. Сутність кібербезпеки держави та основні проблеми її забезпечення. ГЗ 2/2. Загрози в сфері кібербезпеки за стандартами країн-членів НАТО. ГЗ 2/3. Кібернетичні дії та їх особливості. ГЗ 2/4. Основні принципи дій в кіберпросторі та в електронних війнах за стандартами JP 3-12 (Операції в кіберпросторі) та FM 3-12 (Операції в кіберпросторі та електронній війні). С 2/5. Досвід провідних країн світу щодо забезпечення кібербезпеки держави.</p> <p>Тема 3. Планування інформаційної та психологічної операцій за стандартом НАТО АJP.3.10 (Союзна спільна доктрина з інформаційних операцій). Л 3/1. Зміст заходів планування інформаційної операції. ГЗ 3/2. Особливості оперативного планування інформаційної операції. ГЗ 3/3. Основи психологічної операції. ГЗ 3/4. Порядок планування психологічної операції. С 3/5. Фаза VII: Проблеми оцінювання (Evaluation).</p>
<p>Інформаційні джерела</p>	<ol style="list-style-type: none"> 1. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: Підручник. – К.: ДУТ, 2015. – 288 с. 2. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем: підручник. – К.: Видавнича група ВНУ, 2009. – 608 с. 3. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. – Житомир: ЖНАЕУ, 2016. – 636 с. 4. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони. Підручник. – Одеса.: ОНАЗ, 2018 – 228 с.
<p>«Правила гри»</p>	<p>З боку викладача: – забезпечення потреб та запитів ад'юнктів; – подання актуального й необхідного матеріалу; – наповнення дистанційного курсу на платформі Moodle; – дотримання педагогічної справедливості, норм та принципів педагогічної етики, відкритість і щирість у спілкуванні; – забезпечення позитивної й творчої атмосфери на навчальних заняттях.</p> <p>З боку ад'юнкта: – готовність навчатися і змінюватися; – відвідування навчальних занять; – опрацювання лекційного матеріалу; – якісна підготовка до семінарських занять; – доброзичливість, відкритість, щирість, готовність до конструктивної критики; – оригінальність, креативність, ініціативність;</p>

	– дотримання академічної доброчесності.
Додатково	Детальнішу інформацію про навчальну дисципліну “Концептуальні проблеми організації безпеки інформаційного простору Збройних Сил” наведено в робочій програмі навчальної дисципліни