

 <p style="text-align: center;">Національний університет оборони України</p>	<p>СИЛАБУС навчальної дисципліни “КОНЦЕПТУАЛЬНІ ПРОБЛЕМИ ОРГАНІЗАЦІЇ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ ЗБРОЙНИХ СИЛ”</p>
Рівень вищої освіти	Третій (освітньо-науковий), PhD
Спеціальність	126 Інформаційні системи та технології
Статус дисципліни	Основна, реалізується в циклі дисциплін вибору здобувача/здобуття глибинних знань із спеціальності
Мова викладання	Українська (англійська)
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
Лінк на дисципліну	https://adl.mil.gov.ua/course/view.php?id=1353
Оригінальність дисципліни	Авторський курс
Ключові слова	Інформаційна безпека, кібербезпека, захист інформації, кіберпростір, інформаційна операція
 <p style="text-align: center;">Викладач</p>	<p>Волошко Сергій Володимирович, кандидат технічних наук, старший науковий співробітник, професор кафедри комунікаційних технологій та кіберзахисту інституту інформаційно-комунікаційних технологій та кібероборони</p> <p>Сторінка в GoogleScholar: https://scholar.google.com.ua/citations?hl=ru&user=JoVIziQAAAAJ</p> <p>Наукові та навчально-методичні праці за тематикою дисципліни: 1 навчальний посібник, 3 наукові статті</p> <p>Підвищення кваліфікації: “Комунікаційні та інформаційні технології” за програмою НАТО – Україна з перепідготовки військовослужбовців, 28.11.2018 – 12.02.2019.</p> <p>Контактні дані: e-mail: sergijvolosko@gmail.com, кафедра комунікаційних технологій та кіберзахисту, ауд. 2/412</p>
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?	Знання загальних положень щодо забезпечення інформаційної безпеки та кібербезпеки у Збройних Силах України. Знання стану і перспектив розвитку нових способів, технологій та засобів забезпечення інформаційної безпеки та кібербезпеки. Знання і глибоке розуміння інформаційних процесів в органах військового управління, інформаційних системах та мережах. Знання особливостей забезпечення інформаційної безпеки та кібербезпеки у збройних конфліктах і в ході застосування Збройних Сил в операції об'єднаних сил (антитерористичній операції)
Які вміння я розвину?	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. 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). Вміння розробляти та удосконалювати методи і науково-технічні пропозиції для підвищення ефективності забезпечення військ (сил)
Що мене очікує?	Вивчення організації системи заходів щодо забезпечення інформаційної безпеки та кібербезпеки у Збройних Силах України, використання способів, технологій та засобів забезпечення інформаційної безпеки та кібербезпеки
Якого результату я досягну?	Формування фундаментальних теоретичних знань щодо забезпечення інформаційної безпеки та кібербезпеки у Збройних Силах України, використання способів, технологій та засобів забезпечення інформаційної безпеки та кібербезпеки
Де я зможу застосувати отримані знання та вміння?	Під час проведення наукових досліджень. Під час обговорення відповідних тем на наукових конференціях, семінарах, круглих столах, нарадах, дискусіях, суперечках тощо
Зміст навчальної дисципліни	Тема 1. Основи інформаційної безпеки. Л 1/1. Основні положення інформаційної безпеки. ГЗ 1/2. Законодавчий та адміністративний рівні інформаційної безпеки. ГЗ1/3. Організаційний та технічний рівні інформаційної безпеки. ГЗ1/4. Програмно-технічний рівень інформаційної безпеки. Тема 2. Сутність кібербезпеки держави та основні проблеми її забезпечення. Л2/1. Сутність кібербезпеки держави та основні проблеми її забезпечення. ГЗ2/2. Загрози в сфері кібербезпеки за стандартами країн-членів НАТО. ГЗ2/3. Кібернетичні дії та їх особливості.

	<p>ГЗ2/4. 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).</p> <p>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).</p> <p>ЛЗ/1. Зміст заходів планування інформаційної операції.</p> <p>ГЗ 3/2. Особливості оперативного планування інформаційної операції.</p> <p>ГЗ3/3. Основи психологічної операції.</p> <p>ГЗ3/4. Порядок планування психологічної операції.</p> <p>С 3/5. Фаза VII: Проблеми оцінювання (Evaluation)</p>
Інформаційні джерела	<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. Гришук 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.
“Правила гри”	<p>З боку викладача:</p> <ul style="list-style-type: none"> – 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>З боку ад’юнкта:</p> <ul style="list-style-type: none"> – 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; – дотримання академічної доброчесності
Додатково	<p>Детальнішу інформацію про навчальну дисципліну “Концептуальні проблеми організації безпеки інформаційного простору Збройних Сил” наведено в робочій програмі навчальної дисципліни</p>