Освітній компонент	Вибірковий освітній компонент 2**.** **«Забезпечення інформаційної безпеки держави»**
Рівень ВО	перший (бакалаврський) рівень
Назва спеціальності / освітньо-професійної програми	291 «Міжнародні відносини, суспільні комунікації та регіональні студії» / «Регіональна безпека»
Форма навчання	Денна
Курс, семестр, протяжність	2 (3 семестр), 5 кредитів ЄКТС
Семестровий контроль	залік
Обсяг годин (усього: з них лекції/практичні)	150год, з них: лекц. – 10 год, практ. – 20 год
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Кафедра міжнародних комунікацій та політичного аналізу
Автор ОК	**Шуляк Назарій Олександрович**
Короткий опис	
Вимоги до початку вивчення	Базові знання з інформаційно аналітичної діяльності, історії, політичних інституцій.
Що буде вивчатися	Охоплення основ інформаційної безпеки, включаючи різні типи загроз, які можуть поставити під загрозу безпеку даних і систем держави, а також різні стратегії і технології, які можуть бути використані для захисту від цих загроз. Загрози та тенденції кібербезпеки, містить огляд поточного ландшафту загроз, включаючи нові тенденції та нові типи атак, які використовуються для нападів на уряди та інші організації. Управління та оцінка ризиків, буде присвячений процесу виявлення та оцінки ризиків для інформаційної безпеки, а також розробці та впровадженню стратегій управління ризиками для їх зменшення.
Чому це цікаво/треба вивчати	Вивчення дисципліни надасть розуміння різних типів технологій безпеки, які можуть бути використані для захисту інформації та систем, шифрування інформації та відповідне програмне забезпечення. Розпізнавати внутрішні загрози та зосереджуватися на ризиках, які становлять інсайдери, такі як працівники, підрядники та постачальники, які можуть мати доступ до конфіденційної інформації та систем.
Чому можна навчитися (результати навчання)	Загалом, вибірковий освітній компонент надасть здобувачам комплексне розуміння загроз і ризиків, пов’язаних з інформаційною безпекою, а також стратегій, політик і технологій, які можуть бути використані для захисту від цих загроз і забезпечення безпеки конфіденційних даних і критичної інфраструктури.
Як можна користуватися набутими знаннями й уміннями (компетентності)	Знання в даній галузі дозволить керувати процесами виявлення та оцінки ризиків для інформаційної безпеки, а також розробці та впровадженню стратегій управління ризиками для їх зменшення. Використовувати та впроваджувати політику та процедури безпеки які охоплюють розробку та

	впровадження політик і процедур безпеки, включаючи контроль доступу, класифікацію даних, реагування на інциденти та планування безперервності бізнесу.
Інформаційне забезпечення та/або web-покликання	Силабус, статті у фахових наукових виданнях України
Здійснити вибір	