СИЛАБУС
освітнього компоненту (ОК)
«УПРАВЛІННЯ ІНЦИДЕНТАМИ БЕЗПЕКИ»

Назва ОК	Управління інцидентами безпеки
Інформація про ОК	Курс рекомендовано здобувачам ОПП «БІКС»
Тривалість ОК	150 годин (5 кредитів ECTS)
Очікувані результати навчання	Майбутні бакалаври, опановуючи ОК, мають ***знати*:** - загальні проблеми безпеки інформаційних систем; - основні види інформаційних інцидентів, їх відмінності від інших видів інцидентів; - про місце і роль аналізу управління інцидентами в загальному комплексі заходів щодо ОІБ; - методи і засоби управління інформаційними інцидентами; основні міжнародні стандарти і рекомендації по управлінню інформаційними інцидентами; ***уміти***: - вирішувати задачі супроводу (в т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*; - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*; - вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах* на основі моделей управління доступом (мандатних, дискриційних, рольових); - вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*; - забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в *IT* та *SMART-системах*; - вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*; - проводити розслідування інцидентів інформаційної та/або кібербезпеки, базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної та/або кібербезпеки; - забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації. Відповідно до ОПП «БІКС» у процесі вивчення ОК передбачається формування у студентів таких **компетентностей:** **фахові** здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку
Ключові слова	інцидент, вразливість, моніторинг, аудит, реєстрація, реагування, розслідування, модель, політика, управління
Тижневий розклад	аудиторних – 2 самостійної роботи студента – 4

Теми	**Змістовий модуль 1. Побудова системи забезпечення ІБ на основі управління інцидентами ІБ.** *Тема 1* Концептуальний підхід до побудови ефективної системи ІБ. *Тема 2* Поняття та ознаки інциденту ІБ. Місце і роль управління інцидентами в системі забезпечення ІБ організації. *Тема 3* Побудова процесу управління інцидентами. *Тема 4* Розробки та впровадження комплексної системи управління інцидентами інформаційної безпеки *Тема 5*. Система моніторингу подій ІБ. Реагування на інциденти інформаційної безпеки. *Тема 6* Структура та організація системи управління комп'ютерними інцидентами інформаційної безпеки *Тема 7* Система розслідування інцидентів. *Тема 8* Метрики інцидентів. *Тема 9* Використання метрик управління безпекою **Змістовий модуль 2. Реалізація концепції системи управління інформаційними інцидентами.** *Тема 10* Рекомендация МСЭ-Т Е.409. Организация по реагированию на инциденты и обработка инцидентов безопасности. *Тема 11* Обробка інцидентів інформаційної безпеки. *Тема 12* Інтелектуальна система керування інцидентами інформаційної безпеки та підтримки прийняття рішень. *Тема 13* Управління безперервністю бізнесу на основі управління інформаційними інцидентами. *Тема 14* Аналіз стандартів ISO/IEC та української нормативної бази в частині керування інцидентами інформаційної безпеки. *Тема 15* Оцінка затрат компанії на інформаційну безпеку. *Тема 16* Керівництво з обробки інцидентів, пов'язаних з витоком внутрішньої інформації. *Тема 17* Керівництво з обробки інцидентів, пов'язаних з DDoS-атаками та зараженням вірусною програмою Windows-компьютера. *Тема 18* Топ 20 найбільш критичних захисних заходів та засобів
Дата і місце проведення заліку/екзамену	За розкладом
Біографія е-тьютора	**Освіта:** Державний університет телекомунікацій. Магістр за спеціальністю Системи захисту від несанкціонованого доступу, Кваліфікація – науковий співробітник, викладач ВНЗ, інженер у галузі інформаційної безпеки. Диплом: КВ № 37582778, від 30.01.2010 **Науковий ступінь:** Кандидат технічних наук. Диплом ДК №037783 від 29.09.2016р. Спеціальність спеціальністю 21.05.01 "Інформаційна безпека держави". Тема дисертації: «Метод оцінювання стану захищеності інформаційних ресурсів на основі дослідження джерел загроз інформаційній безпеці». **Вчене звання:** немає
Інформація для підтримання зв'язку з е-тьютором	Яніна Володимирівна Рой y.roi@kubg.edu.ua
Попередня підготовка	Знання, вміння і компетенції, сформовані в ході вивчення дисциплін «Теоретичні аспекти захищених інформаційно-комунікаційних

	технологій», «Захист інформації в інформаційно-комунікаційних системах», «Прикладні аспекти аналізу та синтезу політик безпеки», «Стандарти інформаційної та кібербезпеки».
Як навчатися?	Студенти опрацьовують теоретичний матеріал лекцій, підручників, навчально-методичних посібників та інших інформаційних джерел, виконують практичні,лабораторні, семінарські завдання.
Навчальні методи і прийоми, які будуть використовуватися протягом курсу	Проведення лекційних, практичних і семінарських занять.
Навчальні матеріали	Комплект методичних розробок лекційних, практичних і семінарських занять; електронний навчальний курс, методична та наукова література
Необхідне устаткування	Комп'ютери, програмне забезпечення, підключення до мережі Інтернет **Центр дослідження технологій захисту інформаційних ресурсів Лабораторія безпеки інформаційних активів** Університету
Групові/ Індивідуальні види навчальної діяльності	Лекції (*словесні, словесно-наочні, пояснювально-ілюстративні*) Практичні заняття (*ознайомчі, підтверджуючі, частково-пошукові, дослідницькі*) Семінарські заняття (*інтерактивні, репродуктивні, проблемно-прошукові*) Самостійна робота (*пошукові, дослідницькі, проектні, колективної розумової діяльності*)