|  |  |
| --- | --- |
| E:\nubip_logo_new_poisk_18_2.png | **СИЛАБУС ДИСЦИПЛІНИ**  **«Інформаційна безпека держави»** |
| **Ступінь вищої освіти - Бакалавр** |
| **Спеціальність 125 «Кібербезпека»** |
| **Освітня програма «Кібербезпека»** |
| **Рік навчання 1,2 семестр 2,3**  **Форма навчання** денна |
| **Кількість кредитів ЄКТС 8** |
| **Мова викладання** українська |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| **Лектор курсу** | https://nubip.edu.ua/sites/default/files/imagecache/120x160/dsc_7615.jpg **Касаткін Дмитро Юрійович, к.пед.н., доцент (**[**Портфоліо НПП**](https://docs.google.com/document/d/17OLbNsNk0Y9tdyoWP7E5wG7XmQgW_iH1IeZjyXaIR4w/edit#heading=h.cn7fagdotg7g)**)** |
| **Контактна інформація лектора (e-mail)** | **Кафедра комп'ютерних систем і мереж,**  **корпус. 15, к. 207, тел. 5278199**  **e-mail d.kasatkin[@nubip.edu.ua](mailto:d.kasatkin@nubip.edu.ua)** |
| **Сторінка курсу в eLearn** | <https://elearn.nubip.edu.ua/course/view.php?id=2097> |

**ОПИС ДИСЦИПЛІНИ**

В курсі студенти знайомляться з поняттями інформаційна безпеки, як з однією із суттєвих складових частин національної безпеки країни. У сфері інформаційної безпеки знання (в будь-якій формі їх подання) виступають, з одного боку, як об’єкт безпосереднього захисту, а з другого – як фактор забезпечення інтересів людини, суспільства та країни у будь-якій сфері їх життєдіяльності на інформаційному рівні. Під методологічними засадами інформаційної безпеки розуміємо єдність концептуальних, теоретичних і технологічних основ забезпечення на інформаційному рівні безпеки всіх сфер державної і суспільної діяльності (політичної, економічної, соціальної, воєнної, екологічної, духовної та ін.), а також сфер формування, обігу, накопичення і використання інформації (інформаційний простір, інформаційні ресурси, інформаційно-аналітичне забезпечення органів державного управління у всіх різновидах діяльності тощо). Предметом методології інформаційної безпеки є дослідження способів, методів, засобів і каналів реалізації загроз національним інтересам на інформаційному рівні та їх своєчасного виявлення, запобігання і нейтралізації. Метою вивчення навчальної дисципліни «Інформаційна безпека держави» є формування знань про теоретичні основи інформаційної безпеки, особливості забезпечення інформаційної безпеки держави, правила відношення інформації до державної таємниці, конфіденційної інформації, що є власністю держави, недержавної конфіденційної і відкритої інформації що потребує захисту, шляхи побудови систем забезпечення інформаційної безпеки.

**Навчальна дисципліна забезпечує формування ряду загальних компетентностей**:

ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК6. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

ЗК 8. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КФ1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

**У результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме**

ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

**Зробимо курс корисним для вас. Якщо ви будете наполегливо працювати і докладати особливих зусиль, щоб не відставати від матеріалу, ви отримаєте винагороду – як в короткостроковій перспективі, так і в набутті фахових компетентностей. Будь-ласка, широко використовуйте аудиторні заняття, відеоінструкції, вебінари, щоб переконатися, що рухаєтесь за графіком навчання**.

**СТРУКТУРА КУРСУ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Тема** | **Години**  (лекції/  лабора-торні) | **Результати навчання** | **Завдання** | **Оцінювання** |
| **2 семестр** | | | | |
| **Модуль 1. Основні поняття та визначення інформаційної безпеки держави** | | | | |
| Аналіз стану інформаційного простору та інформаційної безпеки держави. | 2/2 | Вміти застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.  Вміти діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.  Вміти готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. | Виконання та захист лабораторних робіт.  Неформальна оn-line освіта на основі Cisco. | **10**  **5** |
| Джерела загроз інформаційній безпеці. | 2/2 | Виконання та захист лабораторних робіт.  Самостійне вивчення онлайн курсу Cisco-Cybersecurity. | **10**  **5** |
| Сутність інформаційної безпеки держави, суспільства та особи. | 2/2 | Виконання та захист лабораторних робіт.  Самостійне вивчення онлайн курсу Cisco-Cybersecurity | **10**  **10** |
| Основи інформаційного протиборства. | 4/4 | Виконання та захист лабораторних робіт.  Самостійне вивчення онлайн курсу Cisco-Cybersecurity. | **10**  **10** |
| Модульний контроль | | | тест в системі  E-Learn | **30** |
| **Модуль 2. Загрози національній безпеці держави та боротьба з ними в інформаційній сфері** | | | | |
| Основні загрози національній безпеці держави в інформаційній сфері. | 4/4 | Вміти застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.  Вміти діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.  Вміти готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. | Виконання та захист лабораторних робіт | **10** |
| Стратегічні цілі та завдання інформаційної боротьби. | 4/4 | Виконання та захист лабораторних робіт. | **10** |
| Державне управління інформаційною безпекою. | 4/4 | Виконання та захист лабораторних робіт. | **10** |
| Національний інформаційний простір. | 4/4 | Виконання та захист лабораторних робіт. Неформальна оn-line освіта на основі Cisco. | **10**  **10** |
| Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. | 4/4 | Виконання та захист лаб. робіт. Неформальна оn-line освіта на основі Cisco. | **10**  **10** |
| Модульний контроль | | | тест в системі  E-Learn | **30** |
| **Всього за 1 семестр** | | | | **70** |
| **Залік** |  |  | тест | **30** |
| **Всього за курс** | | | | **100** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Тема** | **Години**  (лекції/  лабо-раторні) | **Результати навчання** | **Завдання** | **Оцінювання** |
| **3 семестр** | | | | |
| **Модуль 3. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності** | | | | |
| Свобода слова та інформаційна безпека | 2/2 | Вміти впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.  Вміти застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. | Виконання та захист лабораторних робіт.  Неформальна оn-line освіта на основі Cisco. | **10**  **5** |
| Основи державної політики в сфері інформаційної безпеки України | 2/2 | Виконання та захист лабораторних робіт.  Самостійне вивчення онлайн курсу Cisco-Cybersecurity. | **10**  **5** |
| Досвід забезпечення інформаційної безпеки в державах ЄС, США | 2/2 | Виконання та захист лабораторних робіт.  Самостійне вивчення онлайн курсу Cisco-Cybersecurity. | **10**  **5** |
| Модель представлення системи інформаційної безпеки. | 4/4 | Виконання та захист лабораторних робіт.  Самостійне вивчення онлайн курсу Cisco-Cybersecurity. | **10**  **5** |
| Види та властивості інформації як предмета захисту | 4/4 |  | Виконання та захист лабораторних робіт. | **10** |
| Модульний контроль | | | тест в системі  E-Learn | **30** |
| **Модуль 4. Державна політика у сфері телекомунікацій** | | | | |
| Інформаційно-комунікаційні технології та проблеми їхньої безпеки. | 4/4 | Вміти впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.  Вміти застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. | Виконання та захист лабораторних робіт. | **10** |
| Критерії безпеки інформаційних технологій | 4/4 | Виконання та захист лабораторних робіт. Неформальна оn-line освіта на основі Cisco. | **10**  **10** |
| Державна політика у сфері телекомунікацій. Проблеми розвитку захищених телекому-нікацій в Україні та основні шляхи їх розв’язання. | 4/4 | Виконання та захист лабораторних робіт.  Неформальна оn-line освіта на основі Cisco. | **10**  **10** |
| Інформаційна безпека в умовах сучасного стану та перспектив розвитку державності. | 4/4 | Виконання та захист лабораторних робіт. Неформальна оn-line освіта на основі Cisco. | **10**  **10** |
| Модульний контроль | | | тест в системі  E-Learn | **30** |
| **Всього за 1 семестр** | | | | **70** |
| **Екзамен** |  |  | тест, теоретичні питання | **30** |
| **Всього за курс** | | | | **100** |

**ПОЛІТИКА ОЦІНЮВАННЯ**

|  |  |
| --- | --- |
| ***Політика щодо дедлайнів та перескладання:*** | Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний). |
| ***Політика щодо академічної доброчесності:*** | Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних гаджетів). |
| ***Політика щодо відвідування:*** | Відвідування занять є обов’язковим. За об’єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в он-лайн формі за погодженням із деканом факультету) |

**ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ**

|  |  |  |
| --- | --- | --- |
| **Рейтинг здобувача вищої освіти, бали** | **Оцінка національна за результати складання екзаменів заліків** | |
| **екзаменів** | **заліків** |
| 90-100 | відмінно | зараховано |
| 74-89 | добре |
| 60-73 | задовільно |
| 0-59 | незадовільно | не зараховано |