# СИЛАБУС ДИСЦИПЛІНИ «ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ»

**Ступінь вищої освіти – Бакалавр**
**Спеціальність 125 – КІБЕРБЕЗПЕКА**
**Освітня програма «Кібербезпека»**
**Рік навчання 2, семестр 3**
**Форма навчання** денна
**Кількість кредитів ЄКТС 3**
**Мова викладання** українська

| | |
|---|---|
| **Лектор курсу** |  |
| **Контактна інформація лектора (e-mail)** | **МАМЧЕНКО Сергій Миколайович**<br>**Кафедра комп'ютерних систем, мереж та кібербезпеки**<br>**корпус. 15, к. 207, тел. 5278724**<br>**e-mail s.mamchenko@nubip.edu.ua** |
| **Сторінка курсу в eLearn** | **ЕНК (3 семестр)**<br>https://elearn.nubip.edu.ua/course/view.php?id=3831 |

## ОПИС ДИСЦИПЛІНИ

Навчальна дисципліна передбачає вивчення основ національного законодавства в сфері кібербезпеки, міжнародних стандартів та найкращих світових практик щодо забезпечення інформаційної/кібербезпеки, а також основ проведення аудиту систем управління інформаційної безпеки. В ході вивчення дисципліни Ви можете отримати досвід із впровадження систем управління інформаційною безпекою.

Вивчаються наступні питання: структура національного та міжнародного законодавства в сфері інформаційної/кібербезпеки. Організація процесу захисту інформаційних ресурсів організації відповідно до державних (міжнародних) вимог та стандартів, а також відповідно до нормативно-правових документів, внутрішніх стандартів та визначеної політики безпеки організації; напрямки й методи роботи з персоналом, що володіє конфіденційною інформацією; організація процесу визначення ризиків або прогнозування загроз конфіденційності, цілісності, доступності інформаційних ресурсів та рівня їх небезпеки; розробка політики безпеки, впровадження ризик-орієнтованого підходу для вибору заходів із забезпечення інформаційної безпеки підприємства. Організація та управління службою захисту інформації (інформаційної безпеки). Управління інцидентами інформаційної безпеки, забезпечення неперервністю функціонування підприємства. Основні поняття проведення внутрішніх аудитів системи управління інформаційною безпекою.

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

ФК1. 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.

ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

ФК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

ФК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

ФК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

ФК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

ФК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

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

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

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 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної, і/або кібербезпеки;

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

ПРН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;

ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

**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/ лабораторні,) | Результати навчання | Завдання | Оцінювання |
|---|---|---|---|---|
| **1 семестр** | | | | |
| **Модуль 1. Система законодавства в сфері кібербезпеки.** | | | | |
| Система національного законодавства України у сфері кібербезпеки. | **2/4** | Вміти діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. | Теоретичне опитування<br>Тестування<br>Здача лабораторної роботи | **10**<br>**20**<br>**20** |
| Система міжнародних законодавства та стандартів у сфері інформаційної/кібербезпеки. | **2/2** | | Теоретичне опитування<br>Тестування | **10**<br>**10** |
| Модульний контроль | | | Підсумковий тест в ЕНК | **30** |
| **Модуль 2. Системи управління інформаційною безпекою.** | | | | |
| Системи управління інформаційною безпекою. Основні принципи побудови СУІБ. | **2/4** | Знати та 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. | Опитування | **5** |
| Основи управління інформаційними ризиками. | **2/0** | | Опитування | **5** |
| Напрямки побудови СУІБ. Політика ІБ організації. Фізична безпека організації та устаткування. Управління комп'ютерами та мережами. Управління доступом. Вимоги до інформаційних систем. | **2/10** | Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. | Опитування<br>Тестування<br>Здача лабораторної роботи | **5**<br>**25**<br>**15** |
| Управління інцидентами в СУІБ. Питання безперервності функціонування організації. | **2/2** | Здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. | Опитування | **5** |
| Внутрішній аудит СУІБ. | **2/0** | Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних | Тестування | **10** |

| | | | | |
|---|---|---|---|---|
| | | (автоматизованих) системах в ході проведення випробувань згідно з встановленою політикою інформаційної та\або кібербезпеки. | | |
| Модульний контроль | | | Підсумковий тест в ЕНК | **30** |
| **Модуль 3. Впровадження системи управління інформаційною безпекою.** | | | | |
| Методика впровадження СУІБ. | **2/4** | Вміти впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. Здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. | Тестування та опитування. Здача лабораторної роботи. | **5** **10** |
| Розробка документа політики інформаційної безпеки та цілей СУІБ. Управління інформаційними активами. | **2/6** | | Опитування Здача лабораторної роботи. | **5** **10** |
| Впровадження системи управління інформаційними ризиками. | **2/4** | Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. | Здача лабораторної роботи. | **10** |
| Розробка та обґрунтування заходів з обробки та зниженню інформаційних ризиків. | **2/4** | | Здача лабораторної роботи. | **10** |
| Структура документації СУІБ та порядок її розробки. Розробка управлінських процедур. | **2/5** | | Здача лабораторної роботи. | **10** |
| Розробка плану безперервності функціонування організації. Розробка процедур реагування на надзвичайні ситуації. Розробка процедур переходу на аварійний режим. Введення в дію СУІБ. | **2/4** | Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами. | Здача лабораторної роботи. | **10** |
| Модульний контроль | | | Підсумковий тест в ЕНК | **30** |
| **Всього за 1 семестр** | | | | **70** |
| **Екзамен** | | | **Тест, теоретичні питання, задача** | **30** |
| **Всього за курс бали** | | | | **100** |
| **Всього за курс години** | | | | **30/30/48** |

## ПОЛІТИКА ОЦІНЮВАННЯ

| | |
|---|---|
| ***Політика щодо дедлайнів та перескладання:*** | Дедлайни визначені в ЕНК. 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, стажування або відрядження). |
| ***Політика щодо академічної доброчесності:*** | Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних девайсів). |
| ***Політика щодо відвідування:*** | Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line 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 |

## РЕКОМЕНДОВАНА ЛІТЕРАТУРА

**ОСНОВНА**


1. В.А.Хорошко, А.А.Чекатков. Методи та засоби захисту інформації: К. - Юниор, 2003. – 504 с.
2. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997.
3. ДСТУ 3396.0-96.Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.
4. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.
5. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. № 200.
6. НД ТЗІ 1.1-002-99.Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
7. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
8. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
9. НД ТЗІ 3.3-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації» **Додаткова**
10. Положення про державний контроль за станом технічного захисту інформації від 16.05.2007 №87
11. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006.


**ІНФОРМАЦІЙНІ РЕСУРСИ**


12. Електроний навчальний курс на базі Елерн з дисципліни ОЗЗІ https://elearn.nubip.edu.ua/enrol/index.php?id=3831

14.https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi//

15. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “Основи технічного захисту інформації” https://pns.hneu.edu.ua/course/view.php?id=5389