СИЛАБУС ДИСЦИПЛІНИ
«МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ»

Ступінь вищої освіти – Бакалавр
Спеціальність 125 – КІБЕРБЕЗПЕКА
Освітня програма «Кібербезпека»
Рік навчання 2, семестр 3
Форма навчання денна
Кількість кредитів ЄКТС 5
Мова викладання українська

Лектор курсу	**Сагун Андрій Вікторович, к.т.н., доцент (портфоліо)** 
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки, корпус. 15, к. 207, тел. 5278724** **e-mail a.sagun@nubip.edu.ua**
Сторінка курсу в eLearn	**ЕНК (3 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=3970

ОПИС ДИСЦИПЛІНИ

Метою вивчення дисципліни «Методи та засоби захисту інформації» є ознайомлення з основними фізичними принципами, методами та засобами захисту інформації та пошуку розвідувальної апаратури, надання студентам знань з основ захисту інформації, принципів, методів та засобів несанкціонованого одержання інформації, а також створення протидії захисту інформації по каналах, на яких можливі її втрати. Вивчаються наступні питання: засоби несанкціонованого одержання інформації; методи протидії та захисту інформації від її несанкціонованого одержання; канали несанкціонованого одержання інформації; принципи та методи захисту інформації; механізми захисту інформації; методи захисту програмного забезпечення.

Навчальна дисципліна забезпечує формування ряду загальних та фахових компетентностей:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку

СК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

СК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

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

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

ПРН 12. Розробляти моделі загроз та порушника.

ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН 19. . Застосовувати теорії, методи та засоби захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) 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/ Лаборат-орні,)	Результати навчання	Завдання	Оцінювання
3 семестр				
Модуль 1. Комп'ютерні методи і засоби захисту інформації				
Вступ до курсу. Причини, види та канали витоку інформації. Еволюційний розвиток методів та засобів захисту інформації (ЗІ).	**2/2**	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;	Теоретичне опитування.	**5**
Методи та засоби захисту інформації, їх класифікація. Фізичні, апаратні, організаційні, програмні, законодавчі та психологічні засоби захисту	**2/2**	Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних; Виявляти небезпечні сигнали технічних засобів; Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-	Здача лабораторної роботи.	**5**
Захист властивостей інформації при передавання в комп'ютерних мережах. Захист цілісності з використанням алгоритмів підрахунку контрольних сум Ethernet-пакетів	**4/4**		Здача лабораторної роботи.	**5**

		телекомунікаційних (автоматизованих) системах;		
Моделювання вторгнення внаслідок несанкціонованого доступу. Моделі загроз та порушника.	**2/2**	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;	Здача лабораторної роботи.	**5**
Реалізація криптографічних методів захисту (хешування та шифрування) в апаратних засобах ІКС	**4/4**	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.	Здача лабораторної роботи.	**5**
Система електронного документообігу з точки зору кібербезпеки. Захист документаційної інформації та системи електронного документообігу, які підлягають захисту. Роль та функції ЕЦП в захисті.	**6/6**		Здача лабораторної роботи.	**5**
Модульний контроль			Підсумковий тест в ЕНК	**5**
Всього за модуль	**20/20**			**35**
Модуль 2. Організаційні та інженерно-технічні методи та засоби захисту інформації				
Психологічні засоби захисту інформації. Соціальна інженерія та методи боротьби з психологічними методами атаки на властивості інформації	**2/-**	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.	Тестування та опитування.	
Методи захисту віддаленого доступу до інформації. Організація захищених з'єднань	**4/4**		Здача лабораторної роботи.	**5**
Налаштування авторизації до хмарних сховищ електронних документів. Спеціалізовані засоби захисту конфіденційності.	**4/2**		Здача лабораторної роботи.	**5**
Методи забезпечення мережевої безпеки в КС. Мережеві сканери. Використання мережевих сканерів для фіксації втручання в роботу ІКС	**4/3**	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).	Здача лабораторної роботи.	**5**
Налаштування систем блокування та попередження вторгнень (IDS та IPS системи). Міжмережеві екрани.	**4/4**		Здача лабораторної роботи.	**5**
Реалізація та проектування політик безпеки/доступу в інформаційних системах	**4/4**	Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;	Здача лабораторної роботи.	**5**
Управління доступом та система реєстрації подій. Журналювання та аналітика безпеки	**3/4**	Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації	Здача лабораторної роботи.	**5**

		подій, їх аналізу та встановлених процедур захисту;		
Модульний контроль			Підсумковий тест в ЕНК	**5**
Всього за семестр	**25/25**			**70**
Екзамен			**Тест, теоретичні питання, задача**	**30**
Всього за курс	**45/45**			**100**

Неформальна on-line освіта на основі МВОК.

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). В разі здачі лабораторних робіт пізніше запланованих термінів без поважної причини оцінка може бути знижена
Політика щодо академічної доброчесності:	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних пристроїв).
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**	
	Екзаменів	**Заліків**
90-100	Відмінно	-
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	-

Рекомендована література

1. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2010. – 316 с.
2. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ "ПолітрафКонсалтинг", 2010. – 216 с.
3. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510
4. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997.
5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.
6. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.
7. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. №200.
8. НД ТЗІ 1.1-002-99.Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
9. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

10. 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.