СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Ризики інформаційної безпеки»

Ступінь вищої освіти - Бакалавр
Спеціальність «125-Кібербезпека»
Освітня програма «Кібербезпека»
Рік навчання 2, семестр 4
Форма здобуття вищої освіти - денна
Кількість кредитів ЄКТС 4
Мова викладання українська/англійська

Лектор навчальної дисципліни	**Сагун Андрій Вікторович, к.т.н., доцент**  **(портфоліо)**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем і мереж,** **корпус. 15, к. 207, тел. 5278724** **e-mail a.sagun@nubip.edu.ua**
URL ЕНК на навчальному порталі НУБіП України	**ЕНК (4 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=3970

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(до 1000 друкованих знаків)

Метою вивчення дисципліни «Ризики інформаційної безпеки» є формування комплексу знань щодо основ ідентифікації та управління ризиками інформаційної безпеки на підприємствах та організаціях різних форм власності, набуття студентом теоретичних знань та практичних навичок щодо ідентифікації та управління ризиками інформаційної безпеки в інформаційно-телекомунікаційних (автоматизованих) системах в межах встановленої політики безпеки відповідно до рекомендацій нормативних документів серій ДСТУ ISO/IEC 27000 та 31000.

Вивчаються **наступні питання**: основні поняття, терміни і означення теорії та практики управління та ідентифікації ризиків; стратегій та методик управління ризиками (CRAMM, OCTAVE), нормативні документи на міжнародні стандарти по управлінню ризиками в контексті ризик – орієнтованого підходу забезпечення кібербезпеки; експертні методи оцінки ризиків, засоби автоматизованої обробки та керування ризиками.

Компетентності навчальної дисципліни:

Загальні компетентності:

- здатність застосовувати знання у практичних ситуаціях.
- знання та розуміння предметної області та розуміння професії.
- вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
- здатність до абстрактного і системного мислення, аналізу та синтезу

Спеціальні (фахові) компетентності:

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

Програмні результати навчання навчальної дисципліни:

- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
- аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних;
- здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
- здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
- застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
- вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

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/ практичні)	Результати навчання	Завдання	Оцінювання
3 семестр				
Модуль 1. Оцінка та аналіз ризиків та основи управління ризиками відповідно до ISO/IEC				
Основні поняття, терміни і означення загальної теорії ризиків	**2/-**	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.	Опитування	**2**
Класифікація та оцінки ризиків, вимірювання ризиків ІБ. Стандарт методів загального оцінювання ризиків ДСТУ IEC/ISO 31010:2013	**4/4**	Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно - телекомунікаційних систем; Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах	Здача практичної роботи.	**7**
Основи управління ризиками. Методи управління ризиками. Міжнародні стандарти по управлінню ризиками (ISO/IEC 27001:2013)	**2/4**		Здача практичної роботи.	**7**

		реалізації загроз різних класів;		
Ризик – орієнтований підхід забезпечення кібербезпеки та його задачі. Стратегії обробки ризиків. Вимоги до оцінки і обробки ризиків інформаційної безпеки з урахуванням потреб організації, стандарт ISO/IEC 27001:2022	**2/4**	Аналізувати проекти інформаційно - телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних;	Здача практичної роботи	**6**
Оцінка та моделювання ризикованих ситуацій. Калібрування шкали оцінки ризиків з використанням рекомендацій ДСТУ ISO/IEC 27005.	**4/4**		Здача практичної роботи	**7**
Модульний контроль			Підсумковий тест в ЕНК	**6**
Всього за модуль	**14/16**			**35**
Модуль 2. Ризик-орієнтований підхід на підприємстві. Методи оцінки та обробки ризиків з використанням автоматизованих програмних засобів				
Експертні методи оцінки ризиків. Метод Дельфі. Метод бальної оцінки ризиків.	**2/4**	Застосовувати теорії, методи та засоби захисту для забезпечення безпеки інформації в інформаційно - телекомунікаційних системах. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;	Здача практичної роботи	**8**
Система управляння ризиками в загальні концепції Політики інформаційної безпеки підприємства.	**2/-**		Опитування	**2**
Моделі аналізу ризиків інформаційної безпеки. Моделі ALE, SLE. Якісні та кількісні методики оцінювання ризиків.	**2/-**		Опитування	**8**
План реагування на ризики: реалізація заходів з реагування на ризики; оцінка ефективності реалізованих заходів. Керування ризиками у комплексних системах безпеки діяльності банківських та фінансово-кредитних установ.	**4/-**	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно - телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;	Опитування	**9**
Системи автоматизованого оцінювання та керування ризиками. Програмні продукти для аналізу ризиків інформаційної безпеки: CRAMM, RiskWatch.	**4/6**		Здача практичної роботи.	**2**
Ризик-менеджмент. Документування в систем управління ризиками.	**2/4**	Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.	Здача практичної роботи.	
Модульний контроль			Підсумковий тест в ЕНК	**6**
Всього за семестр	**16/14**			**35**
Екзамен			Тест, теоретичні питання, задача	30
Всього за курс	**30/30**			**100**

Неформальна on-line освіта на основі MBOK.

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 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**	
	Екзаменів	**Заліків**
90-100	Відмінно	-
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	-

Рекомендована література

1. Ю. Лісовська. Книга Кібербезпека. Ризики та заходи. – Вид-во «Кондор», 2019. – 272 с. ISBN 978-617-7729-49-4.
2. Гуменюк В. Я. Управління ризиками : навч. посіб. / В. Я. Гуменюк, Г. Ю. Міщук, О. О. Олійник. – Рівне : НУВГП. - 2009. 156 с.
3. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. - К.: ЦНЛ, 2003. - 188 с.
4. Василевич Л.Ф. Юртин І.І. Прийняття рішень за умов конфлікту та невизначеності середовища. Навчальний посібник – К. : Київ. ун-т ім.. Б. Грінченка. 2013. 128 с.