Волинський національний університет імені Лесі Українки
Кафедра комп'ютерних наук та кібербезпеки
СИЛАБУС
нормативної навчальної дисципліни
ТЕОРІЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Інформаційна безпека (2020 р.)
Форма навчання	Денна
Розробник (викладач)	Прус Руслана Богданівна, кандидат технічних наук
Контактна інформація	prus.ruslana@vnu.edu.ua
Програма навчальної дисципліни	Програма навчальної дисципліни розміщена на сторінці кафедри комп'ютерних наук та кібербезпеки на офіційному сайті ВНУ імені Лесі Українки
Семестр, курс	4 семестр, 2 курс
Обсяг дисципліни	Загальний обсяг: 120 годин, 4 кредити Аудиторних занять: 52, з них 20 лекції, 32 лабораторні роботи Самостійна робота: 59 години Консультації: 9 год.
Форма контролю	Екзамен
Час занять	Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Мова навчання	Українська
Анотація дисципліни	Даний курс знайомить студентів із основними фундаментальними поняттями і законами теорії ризиків для їх використання в сучасних кіберсистемах; принципами побудови алгоритмів оцінки ризиків інформаційної безпеки, основних стандартів оцінки ризиків та побудови моделі загроз і моделі порушника; основним математичним апаратом та законами оцінки ризиків у професійній діяльності; програмними засобами, які реалізують основні алгоритми оцінки ризиків для вирішення типових задач захисту інформації; процедурами управління інцидентами.
Мета вивчення дисципліни	Мета навчальної дисципліни полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного управління ризиками інформаційної безпеки, необхідних для подальшої роботи та навчанні застосуванню методів та засобів оцінки ризиків в умовах широкого використання сучасних методів інформаційної безпеки. Основними завданнями вивчення дисципліни «Теорія ризиків інформаційної безпеки» є: - надати вичерпну та актуальну інформацію про основні фундаментальні поняття і закони теорії ризиків для їх використання в сучасних кіберсистемах; - сформувати у студентів навики побудови алгоритмів оцінки ризиків інформаційної безпеки, розуміння основних стандартів оцінки ризиків та їх використання в задачах захисту інформації; - сформувати у студентів уміння розуміти та використовувати основний математичний апарат та закони оцінки ризиків у

	професійній діяльності; - сформувати у студентів навики програмно реалізовувати основні алгоритми оцінки ризиків для вирішення типових задач захисту інформації; - сформувати у студентів навики виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
Результати навчання	*Загальні компетентності:* Здатність застосовувати знання у практичних ситуаціях. (ЗК 1). Знання та розуміння предметної області та розуміння професії. (ЗК 2). Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.. (ЗК4). Здатність до пошуку, оброблення та аналізу інформації. (ЗК 5). *Фахові компетентності:* Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. (ФК 8). Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою. (ФК 9) Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібезбезпеки. (ФК 12). *Програмні результати навчання:* Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. (ПРН 2) 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 4) Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. (ПРН 5) 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. (ПРН 29) Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. (ПРН 33) Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. (ПРН 42) Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. (ПРН 46)
	• Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. • 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. • Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. • Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

Структура навчальної дисципліни

Назви змістових модулів і тем	Усього	Лек.	Лаб.	Сам. роб.	Конс.	Бали
1	120	20	32	59	9	100
Змістовий модуль 1. Основні положення оцінки та аналізу ризиків інформаційної безпеки						
Лекція 1. Управління ризиками інформаційної безпеки.	4	2		2		
Лабораторна робота 1. Розрахунок ризику інформаційної безпеки на основі аналізу загроз та порушників	4		2	2		2
Лабораторна робота 2. Аналіз вразливостей програмних продуктів	5		2	2	1	4
Лекція 2. Методологія аналізу та оцінки ризиків	5	2		2	1	
Лекція 3. Ідентифікація порушника та її роль при оцінці ризиків	5	2		2	1	
Лабораторна робота 3. Побудова моделі загроз	4		2	2		4
Лабораторна робота 4. Побудова моделі порушника	4		2	2		4
Лекція 4. Методи оцінки ризиків за міжнародними стандартами	5	2		2	1	
Лабораторна робота 5. Методики оцінки ризиків інформаційної безпеки	6		4	2		4
Лабораторна робота 6. Кількісна оцінка ризиків інформаційної безпеки	4		2	2		4
Разом за модулем 1	**46**	**8**	**14**	**20**	**4**	22
Змістовий модуль 2. Практичні аспекти управління ризиками у кібербезпеці						
Лекція 5. Теорія прийняття рішень та моделювання систем захисту	5	2		2	1	
Лабораторна робота 7. Критерії прийняття оптимальних рішень в задачах інформаційної безпеки	4		2	2		2
Лекція 6. Математичне моделювання у задачах інформаційної безпеки	5	2		2	1	
Лабораторна робота 8. Політика контролю доступу та вимоги до паролів	6		2	4		4

Лекція 7. Процес оцінки ризиків у системах управління інформаційною безпекою	4	2		2		
Лабораторна робота 9. Розробка реєстру ризиків	8		4	4		4
Лекція 8. Експертні методи при оцінці ризиків у системах управління інформаційною безпекою	5	2		2	1	
Лабораторна робота 10. Аналіз витрат на управління інцидентами ІБ	4		2	2		4
Лекція 9-10. Основні принципи процесу управління інцидентами інформаційної безпеки	9	4		4	1	
Лабораторна робота 11. Виявлення та реагування на інциденти інформаційної безпеки	6		4	2		4
Разом за модулем 2	**56**	**12**	**14**	**26**	4	18
Модульна контрольна робота №1	6		2	4		10
Модульна контрольна робота №2	6		2	4		10
Екзамен	6			5	1	40
Разом за 4 семестр:	**120**	**20**	**32**	**59**	9	100

Оцінювання

При вивченні дисципліни студент виконує такі види робіт: опрацювання теоретичного матеріалу та виконання лабораторних робіт, виконання індивідуальних завдань, написання тестів.

Рівень знань студента оцінюється в балах, фіксується в журналі після вивчення змістового модуля. Підсумкова оцінка за національною шкалою за семестр заноситься в заліково-екзаменаційну відомість.

Усі види навчальної діяльності студента оцінюються певною кількістю балів. Підсумковий контроль здійснюється у формі екзамену. Сумарна кількість балів, яку студент отримує при засвоєнні змістових модулів за 100-бальною шкалою, визначає його підсумкову оцінку.

Дисципліна складається з двох змістових модулів. Підсумкова оцінка за 100-бальною шкалою складається із сумарної кількості балів за:

1. поточне оцінювання (максимум 40 балів);
2. екзамен (максимум 60 балів).

Поточний контроль, який має на меті перевірку рівня знань студента, здійснюється викладачем упродовж семестру у межах змістових модулів. Поточний контроль включає оцінку поточної роботи студента у ході виконання лабораторних робіт. Максимальна кількість балів за результатами поточного контролю становить 40 балів.

Підсумковий контроль, який здійснюється викладачем, має на меті перевірку рівня знань студента під час виконання екзаменаційного тесту, виконання практичного завдання та усної відповіді. Максимальна кількість балів, яку студент може набрати за екзамен, становить 60 балів, з яких по 10 балів – це оцінка за кожну із двох модульних контрольних робіт.

Поточний контроль (мах = 40 балів)		Модульний контроль/екзамен (мах = 60 балів)			Загальна кількість балів
Змістовий модуль 1	**Змістовий модуль 2**	**МКР 1**	**МКР 2**	**Екзамен**	
20	20	10	10	40	100

Підсумковий контроль

Екзамен складається з трьох частин: 1) написання екзаменаційного тесту (максимум – 20 балів); 2) виконання практичного завдання (максимум 10 балів) та 3) усна відповідь (максимум – 10 балів).

В оцінці знань студентів враховується:

1) достатність обсягу відповіді (повна, недостатньо повна, неповна);

2) обізнаність з основними поняттями, принципами, законами, правилами навчальної дисципліни;

3) логічність викладу матеріалу;

4) обґрунтованість власних міркувань;

5) уміння інтегрувати та диференціювати знання теоретичного матеріалу та застосовувати їх при виконанні практичних завдань.

Відповідь вважається *повною* (*40 балів*), якщо студент повністю оволодів матеріалом, обізнаний з усіма поняттями і термінами навчального курсу і адекватно оперує ними під час відповідей на поставлені питання, а також посилається на наукові дослідження з навчальної дисципліни, ознайомлений зі спеціальною літературою; демонструє здатність аналізувати факти, аргументувати власні судження теоретичними і фактичними положеннями, підсумувати сказане висновками.

Відповідь вважається *недостатньо повною* (*36 балів*) за умов непоганого володіння знаннями з навчального предмету. Відповідь студента має бути правильною й обгрунтованою. Студент повинен продемонструвати знання теоретичного матеріалу, навички самостійної навчально-пізнавальної діяльності, здатність викладати матеріал в певній логічній послідовності. Допускаються незначні помилки, які не впливають на загальне розуміння викладеного матеріалу.

Відповідь вважається *неповною* (*32 бали*), якщо продемонстровані знання з предмету носять фрагментарний і поверхневий характер. Теоретичні і фактичні знання відтворюються репродуктивно, без глибокого осмислення, аналізу, порівняння, узагальнення. Студент обізнаний з літературними джерелами з навчальної дисципліни, але не може дати достатньо критичної їх оцінки; допускає суттєві помилки, які порушують логіку викладення матеріалу.

Екзамен вважається *нескладеним (нижче 24 балів),* за умов неправильної або неповної відповіді, яка свідчить про нерозуміння поставленого завдання. Студент не володіє понятійно-категоріальним апаратом, необізнаний з джерельною базою з навчальної дисципліни і допускає грубі помилки у викладенні матеріалу.

Політика викладача щодо студента

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загальноприйнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування.

Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу.

Політика щодо академічної доброчесності

Під час навчання учасники освітнього процесу зобов’язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності.

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання студенти не користуються забороненими засобами (мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси), самостійно виконують запропоновані завдання.

Політика щодо дедлайнів та перескладання

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона вивчають теоретичний матеріал самостійно використовуючи навчальні посібники, конспекти лекцій, виконують всі завдання для аудиторних занять, всі домашні завдання. Прозвітуватися про виконання завдань можна у встановлені викладачем терміни під час консультацій.

Перескладання модулів відбувається із дозволу викладача за наявності поважних причин (наприклад, лікарняний).

Рекомендована література та інтернет-ресурси

1. Information technology. Security techniques. Information security management systems – Requirements: ISO/IEC 27001:2017
2. Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів: ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT)
3. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. — [Чинний від 28.04.1999]. — К.: ДСТСЗІ СБУ, 1999. — No 22. — (Нормативний документ системи технічного захисту інформації): https://tzi.com.ua/downloads/1.1-003-99.pdf
4. Nagle F., Ransbotham S., Westerman G. *The Effects of Security Management on Security Events*, WEIS, 2017.
5. NIST (National Institute Of Standards And Technology). 1995. *An Introduction to Computer Security: The NIST Handbook*. (Special Publication 800-12).
6. CERT Exercises Handbook, *Cost of ICT incident calculation*.
7. CERT Exercises Toolset, *Cost of incident handling*.
8. Браіловський М.М., Лазарев Г.П., Хорошко В.О. Захист інформації у банківській діяльності. - К.: ТОВ «ПоліграфКонсалтинг», 2004. - 216 с.
9. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. – К.: ЦНЛ, 2003. – 188 с.
10. Катренко А.В., Пасічник В.В., Пасько В.П. Теорія прийняття рішень. – К.: Видавнича група BHV, 2009. – 448с.
11. Саати Т.Л. Принятие решений. Метод анализа иерархий: Пер. с англ. – М.: Радио и связь, 1993. – с. 320.
12. Івченко І.Ю. Моделювання економічних ризиків і ризикових ситуацій. – К.: Центр учбової літератури, 2007. – 344 с.
13. Левченко Є.Г., Прус Р.Б., Швець В.А. Економіка інформаційної безпеки: лабораторний практикум. – К.: НАУ, 2011. – 32 с.

Силабус навчальної дисципліни, затверджено на засіданні кафедри

Комп'ютерних наук та кібербезпеки
протокол № 3 від 05.10.2020р.

Завідувач кафедри:  Сачук Ю.В.