МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Волинський національний університет імені Лесі Українки

Факультет інформаційних технологій і математики

СИЛАБУС

«Теорія ризиків»

нормативної навчальної дисципліни

підготовки бакалавра

галузь знань 12 Інформаційні технології

спеціальність 125 Кібербезпека та захист інформації

освітньо-професійна програма Кібербезпека та захист інформації

Луцьк – 2023

Силабус навчальної дисципліни «Теорії ризиків» підготовки бакалавра, галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека та захист інформації за освітньо-професійною програмою Кібербезпека та захист інформації .

Розробник: Лаптєв О. А., професор кафедри комп'ютерних наук та кібербезпеки, доктор технічних наук, старший науковий співробітник,

Погоджено
Гарант освітньо-професійної програми:  Глинчук Л.Я.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 2 від 28 вересня 2023 р.

Завідувач кафедри:  Гришанович Т. О.

1.Опис навчальної дисципліни

Таблиця 1

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td>Денна форма навчання</td><td rowspan="10">12 Інформаційні технології

125 Кібербезпека та захист інформації

Кібербезпека та захист інформації</td><td>Нормативна</td></tr>
<tr><td rowspan="6">Кількість годин/кредитів 120/4</td><td>Рік навчання 2</td></tr>
<tr><td>Семестр 3-ий</td></tr>
<tr><td>Години:120</td></tr>
<tr><td>Кредити: 4</td></tr>
<tr><td>Лекцій: 46 год.</td></tr>
<tr><td>Лабораторні роботи : 62 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Самостійна робота 4 год.</td></tr>
<tr><td>Консультації: 8 год.</td></tr>
<tr><td>Форма контролю: екзамен</td></tr>
<tr><td>Мова навчання</td><td>українська</td></tr>
</table>

II. Інформація про викладача

ПІП: Лаптєв Олександр Анатолійович
Науковий ступінь: доктор технічних наук
Вчене звання: старший науковий співробітник
Посада: професор кафедри комп'ютерних наук та кібербезпеки
Контактна інформація (номер мобільного зв'язку, електронна адреса): +380674348001, Alaptev64@ukr.net
Дні занять (посилання на електронний розклад):
https://us04web.zoom.us/j/7639442912?pwd=GQ7a6Mq99IamC2mMAMzzh8EF016gEj.1

III. Опис дисципліни

1. Анотація курсу:

Навчальна задача дисципліни «Теорія ризиків» полягає у підвищенні рівня знань здобувачів з теорії і практики інформаційної безпеки, набуття вмінь і навичок з виявлення ризиків витоку інформації, їх блокування, створенні та впровадженні систем управління

ризиками, в знанні основ організації та порядку виконання робіт із створення систем захисту інформації від ризиків інформаційної безпеки телекомунікаційних систем залежно від характеру об'єкта захисту.

2. Пререквізити/постреквізити

Пререквізити: Базові знання інформаційних технологій та захисту інформації

Постреквізити: Знання та вміння є базовими для вивчення наступних навчальних дисциплін.

3. Мета дисципліни – сформувати у здобувачів теоретичних знань та практичних навичок самостійної роботи з забезпечення управління ризиками на об'єктах інформаційної діяльності на основі нормативно-правових документів, національних та міжнародних стандартів. Дати здобувачам поглиблені знання в опануванні загальних теоретичних знань та практичних навичок щодо розробки типової стратегії і організації системи управління ризиками інформаційної безпеки..

4. Результати навчання (компетентності).

Знання теоретичних основ та вміння свідомого поводження з інформацією в умовах використання сучасних інформаційно-комунікаційних засобів та враховування отриманих знань у практичної діяльності за обраної спеціальності.

Інтегральна компетентність: Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у сфері захисту інформації та кібербезпеки.

Загальні компетенції:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
ЗК 2. Знання та розуміння предметної області та розуміння професії.
ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.
ЗК 6. 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.

Спеціальні компетенції:

ФК 1. 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 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.
ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою.
ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Володіти елементарними навичками програмування, навичками використання математичних методів в інформаційних системах та роботи в мережі, дискретної математики, електротехніки та електроніки, теорії алгоритмів.

4. Завдання (навчальні цілі) навчальної дисципліни– забезпечення стабільних базових теоретичних знань, теорії і практики щодо управління інформаційною та кібернетичною безпекою на основі існуючих технологій та програмних продуктів**.**

Сприяти ефективному формуванню у здобувачів наступних професійних компетентностей:

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

ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
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.
ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

5. Структура навчальної дисципліни

№ п/п	Назва теми*	Кількість годин			
		Лекції	**П.р.**	**Л.р.**	**С. р.**
Змістовий модуль 1 «Нормативно-правові акти теорії ризиків інформаційної безпеки»					
1	Тема 1. Загальні положення та вимоги в частині організації робіт із теорії ризиків.	2		6	
2	Тема 2. Правові підстави та основні положення щодо створення систем управління ризиками в Україні	4		4	
3	Тема 3. Оцінка ризиків при захисті інформації в АС від НСД.	4		6	
4	Тема 4. Ризики витоку інформації в АС технічними каналами	4		4	
5	Тема 5. Запобігання проблем захисту інформації в АС від ризиків руйнування каналами спеціального впливу.	4		6	1
6	Тема 6. Порядок проведення робіт зі створення систем управління ризиками інформаційної безпеки	4		4	1
	Всього за МК-1	**22**		**30**	**2**
Змістовий модуль 2 «Побудова системи управління ризиками інформаційної безпеки»					
7	Тема 7. Технічне завдання на створення системи управління ризиками в АС.	4		6	
8	Тема 8. Особливості проектування систем для АС різних класів. Оцінка ефективності та оптимізація.	6		6	1
9	Тема 9. Перспективні напрями розвитку комплексу ЗІ в розподілених обчислювальних середовищах (РОС).	4		8	
10	Тема 10. Випробування систем виявлення ризиків захисту інформації.	6		6	1
11	Тема 11. Введення систем в дію.	4		6	
	Всього за МК-2	**24**		**32**	**2**
	Консультація		**8**		
	Всього за навчальною дисципліною	**46**	**8**	**62**	**4**

Загальний обсяг **120** *год.,* в тому числі:
Лекцій **–46** *год.*
Лабораторні – **62** *год*
Консультації**– 8** *год*
Самостійна робота **– 4** *год.*

8. Питання до екзамену

1. Які головні задачі захисту інформаційних технічних засобів?
2. Які вам відомі підходи до класифікації загроз безпеці інформації?
3. Порівняйте їх між собою з огляду найбільшої відповідності практичним потребам створення систем захисту інформації.
4. Загрози інформаційної безпеки. Загальний процес оцінки ризиків інформаційної безпеки.
5. Кількісні оцінки інформаційних ризиків.
6. Нормативна та законодавча база в оцінці ризиків інформаційної безпеки.
7. Сутність процесу управління інформаційними ризиками.
8. Концепції та методи загального оцінювання ризиків.
9. Аналіз ризиків в системі управління інформаційною безпекою.
10. Визначення пар загроза/вразливість та їх оцінка в рамках оцінки ризиків інформаційної безпеки.
11. Методика оцінки ризиків NIST 800-30 управління ризиками системи інформаційних технологій.
12. Методики оцінки ризиків CRAMM.
13. Методика оцінки ризиків FAIR.
14. Методи оцінки ризиків Risk Watch.
15. Методи оцінки ризиків COBRA.
16. Охарактеризуйте основні принципи системної класифікації загроз безпеці інформації.
17. Наведіть класифікаційну структуру ризиків несанкціонованого витоку інформації.
18. Порівняння методів оцінки ризиків FAIR, NIST 800-30, CRAMM, Risk Watch, COBRA.
19. Наведіть відомі вам методи і засоби контролю акустичної інформації.
20. Розкрийте зміст методів контролю інформації технічними засобами в каналах телефонного зв'язку.
21. Порівняння методів оцінки ризиків NIST, OCTAVE, MESARI, IRAM, MAGERIT.
22. Охарактеризуйте основні способи запобігання витоку інформації по технічних каналах.
23. Сформулюйте основні концептуальні положення теорії захисту інформації.
24. Розкрийте зміст функції захисту інформації. Які з функцій утворюють повну множину функцій захисту?
25. Сформулюйте завдання захисту і назвіть десять класів завдань, що створюють репрезентативну множину задач захисту.
26. Приведіть класифікацію засобів захисту інформації. Які переваги і недоліки програмних, апаратних та організаційних засобів захисту інформації?
27. Як впливають показники інформації, що захищається, на структуру і підходи до проектування системи захисту інформації?
28. Розкрийте зміст короткострокового, середньострокового і довгострокового управління ризиків захисту інформації.
29. Сформулювати задачу оптимального вибору методів захисту від ризиків витоку інформації для кожного конкретного об’єкта і для системи в цілому.
30. Розкрити критерій вибору засобів і методів захисту від ризиків руйнування інформації.
31. Розкрити задачу мінімізації вартості та ефективності забезпечення систем захисту об’єкта.
32. Розкрити задачу мінімізації вірогідності злому усіх методів, які використовуються для захисту об’єкта.
33. Розкрийте поняття загрози інформаційної безпеки. Які основні напрями захисту інформації?
34. Класифікація загроз інформаційної безпеки за компонентами інформаційних систем, на які вони націлені.
35. Класифікація загроз інформаційної безпеки за характером впливу

36. Класифікація загроз інформаційної безпеки за розміщенням їх джерела. Які основні види загроз безпеки інформаційним технологіям?

37. Основні техногенні передбачувані та непередбачені загрози інформаційній системи

38. Яку систему складають дестабілізуючі чинники відповідно до технології і функціонування інформації?

39. Методи оцінки ризиків OCTAVE.

40. Привести структуру каналу витоку інформації та дати характеристику середовищу передачі інформації.

41. Якими видами можуть бути представлені природні канали витоку ?

42. Дайте характеристику каналам витоку інформації, які створені закладними пристроями? Які основні тенденції та шляхи розвитку закладних пистроїв?

43. Завдання Служби захисту інформації.

9. Політика оцінювання

Здобувач має виконати у повному обсязі усі види діяльності із навчальної дисципліни «Нормативно-правове забезпечення інформаційної безпеки», бути присутніми на аудиторних заняттях. Якщо здобувач відсутній на занятті, він може надіслати виконане семінарське заняття у письмовому вигляді. Претендувати на максимальну кількість балів можна, якщо семінарське виконане у вигляді презентацій, використані нові актуальні наукові джерела, робота є авторською, без порушень авторських прав.

Освітній процес відповідає «Положенню про поточне та підсумкове оцінювання знань студентів Волинського національного університету імені Лесі Українки» від 11 вересня 2020 р. (https://bit.ly/39In2ac). Іспит виставляється автоматично за умови, якщо студент виконав усі види навчальної роботи та отримав не менше ніж 75 балів зі 100 можливих.

Вирішення спірних питань у галузі академічної доброчесності здійснюється на підставі Положення про систему запобігання та виявлення академічного плагіату у науково-дослідній діяльності здобувачів вищої освіти і науково-педагогічних працівників Східноєвропейського національного університету імені Лесі Українки (від 10 лютого 2017 р.) (https://bit.ly/3lNJD7N).

Конфліктні ситуації вирішуються згідно Положення про порядок і процедури вирішення конфліктних ситуацій у Волинському національному університеті імені Лесі Українки (https://bit.ly/33MTIM).

Згідно Положення про академічну мобільність студентів (https://bit.ly/3oMzMkk), власне право неформальну освіту, здобувач може отримати найвищу кількість балів за виконання ІНДЗ, якщо взяв участь у тренінгу, конференції, науковому семінарі, проблемній групі та ін.

Здобувач вчасно здає усі види робіт. Викладач інформує про терміни здачі контрольних робіт та виконання ІНДЗ.

Здобувач має можливість скласти іспит згідно розкладу заліково-екзаменаційної сесії, має право скласти іспит повторно, а також скласти іспит комісії, у яку входять представники кафедри та деканату. Якщо за ці три можливості іспит не складено, здобувач виключається зі складу студентів ВНУ імені Лесі Українки. В університетських положеннях є право на поновлення і проходження повторного проходження навчальної дисципліни.

9.1. Розподіл балів, які отримують студенти

Методи навчання: усне опитування, інтерактивні методи навчання, лабораторні заняття, самостійна робота і екзамен.

Засоби діагностики успішності: лабораторні заняття (30 балів), бонусні бали за активність (10), самостійна робота (30 балів), екзамен (40 балів).

Поточний контроль (мах – 30 балів) Лабораторні заняття	Самостійна робота (мах – 30 балів)	Екзамен (мах – 40 балів)	Загальна кількість балів
30 годин лабораторних занять (мах 30 балів) + 10 балів за актив-	67 годин (мах 30 балів)	(мах 40 балів)	100

ність			

10. Шкала оцінювання (національна та ECTS)

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсової роботи (проекту), практики	для заліку
90-100	**A**	**Відмінно**	**Зараховано**
82-89	**B**	**Добре**	
75-81	**C**		
67-74	**D**	**Задовільно**	
60-66	**E**		
1-59	**Fx**	**Незадовільно**	**Незараховано**

РЕКОМЕНДОВАНІ ДЖЕРЕЛА

1. Закон України. Про основні засади забезпечення кібербезпеки України. Введено в дію постановою Верховної Ради України від 05.10. 2017 р. № 45, ст.403.
2. ISO/IEC 11770-3 Information Technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques. January 2007.
3. ISO/IEC 14888-3 Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based Mechanisms. June 2006.
4. Івченко І.Ю. Економічні ризики: Навчальний посібник. – К.: ЦНЛ, 2004. – 304 с.
5. Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process (en). The Software Engineering Institute.
6. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 c.
7. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. К. ДУТ. 2020 – 126 с. https://dut.edu.ua/ua/lib/2/category/96/view/2031
8. О.А. Лаптєв. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. Міленіум. 2020 – 326 с. УДК 004.056.53. ISBN 987-966-8063-79-3. https://www.dut.edu.ua/uploads/l_2162_16683938.pdf

Додаткова література:

1. Богуш В.М., Кудін А.М. Моніторинг і аудит систем інформаційної безпеки. К.: ДУІКТ, 2006, – 340 с.
2. Указ Президента України №446/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"
3. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджено наказом ДСТСЗІ СБ України від 09.02.2001 № 2.
4. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі Затверджено наказом ДСТСЗІ СБ України від 08.11.05.

Додаткові джерела:

1. A.O. Korchenko, V.O. Breslavskyi, S.P Yevseiev, N.K. Zhumangalieva, A.O. Zvarych, S.V. Kazmirchuk, O.A. Kurchenko, O.A. Laptiev, O. V. Severinov, S. S. Tkachuk. Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. Eastern-European journal of enterprise technologies. Vol.1№2 (109), 2021 pp. 14–23. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2021.225346.

2. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615.