МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Кафедра Комп'ютерної інженерії та інноваційних технологій

Введено в дію наказом ректора

Міжнародного гуманітарного

університету від 30. [illegible] № [illegible]

Ректор _____ К.В. Громовенко

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ІНФОРМАЦІЙНА БЕЗПЕКА ІННОВАЦІЙНОЇ ДІЯЛЬНОСТІ

Галузь знань — 12 Інформаційні технології

Спеціальність — 125 «Кібербезпека та захист інформації»

–

Назва освітньої програми — «Кібербезпека»

Рівень вищої освіти — другий (магістерський) рівень

Одеса - 2024 рік

Робоча програма затверджена на засіданні кафедри комп'ютерної інженерії та інноваційних технологій протокол № 1 від 29.08.24 року.

Розробники і викладачі	Контактний тел.	E-mail
Професор кафедри Комп'ютерної інженерії та інноваційних технологій **Радівілова Тамара Анатоліївна**	+380951609153	tamara.radivilova@gmail.com
Доцент кафедри комп'ютерної інженерії та інноваційних технологій, кандидат технічних наук, доцент **Йона Лариса Григорівна**	+380677463777	yonalarysa66@gmail.com

Завідувач кафедри комп'ютерної інженерії та інноваційних технологій, к.т.н., доцент _____ Лариса ЙОНА

Гарант освітньої програми к.т.н., доцент, _____ Лариса ЙОНА

Узгоджено
Начальник навчального відділу _____ Лариса РАЙЧЕВА

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="10">Кількість кредитів – 4, загальна кількість годин – 120

Мова навчання – українська</td><td rowspan="10">Галузь 12 – Інформаційні технології
Спеціальність – 125 «Кібербезпека та захист інформації»

Рівень вищої освіти – другий (магістерський) рівень</td><td colspan="2">обов’язкова</td></tr>
<tr><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">2-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>2-й</td><td>2-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>22 год.</td><td>6год</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>22 год.</td><td>6 год</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>год.</td><td>год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>76 год.</td><td>108год</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>залік</td><td>залік</td></tr>
</table>

Дисципліна **«Інформаційна безпека інноваційної діяльності»** формує у здобувачів необхідний обсяг теоретичних і практичних знань про основні технології, що реалізуються концепцією захисту інформації, яка зберігається та передається у телекомунікаційних системах та мережах від порушення її властивостей, а саме конфіденційності, цілісності та доступності, надання знань фахівцям з сучасних методів захисту інформаційного середовища інноваційних підприємств, тенденцій в галузі захисту інноваційної діяльності, аналіз загроз та ризиків витоку конфіденційної інформації для забезпечення конкурентних переваг інноваційних підприємств, особливостей формування і роботи систем інформаційної безпеки в інноваційних підприємствах та організаціях.

Метою викладання навчальної дисципліни Інформаційна безпека інноваційної діяльності є забезпечення здобувачів знаннями з питань попередження, прогнозування та мінімізації втрат від несанкціонованого доступу до конфіденційної інформації при інноваційній діяльності у системах комунікацій з урахуванням сучасного стану та перспективних напрямів розвитку систем та технологій захисту інформації; сформувати у здобувача здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Передумови для вивчення дисципліни – знання і вміння, отримані студентом при вивченні навчальних дисциплін бакалаврської підготовки.

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Інформаційна безпека інноваційної діяльності» формуються наступні компетентності із передбачених освітньо-професійною програмою «Кібербезпека» зі спеціальності 125 Кібербезпека.

Інтегральна компетентність

ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Здатність проводити дослідження на відповідному рівні.

Фахові компетентності

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Програмні результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та

критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.

РН21. Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

Заплановані результати навчання за навчальною дисципліною

У результаті вивчення цієї навчальної дисципліни студент має набути такі компетентності.

Знати:

- основи державного регулювання інноваційної діяльності в Україні;

- загрози та ризики витоку конфіденційної інформації для забезпечення конкурентних переваг інноваційних підприємств;
- методи захисту конфіденційної інформації при інноваційній діяльності;
- сучасні тенденції в галузі захисту інформації інноваційного підприємства;
- засоби одержання несанкціонованого доступу до конфіденційної інформації;
- організацію системи промислової та економічної контррозвідки в інноваційних організаціях;
- основні положення політики інформаційної безпеки при інноваційної діяльності;
- основні функції служби захисту інформації інноваційної організації;
- особливості моніторингу системи інформаційної безпеки в інноваційних організаціях.

Вміти:

- враховувати загрози та ризики витоку конфіденційної інформації з метою забезпечення конкурентних переваг інноваційної діяльності;
- використовувати основні методи захисту конфіденційної інформації при інноваційній діяльності;
- використовувати сучасні тенденції в галузі захисту інформації інноваційного підприємництва;
- враховувати засоби одержання несанкціонованого доступу до конфіденційної інформації;
- враховувати особливості нормативно-правового регулювання інноваційної діяльності;
- враховувати організацію системи промислової та економічної контррозвідки в інноваційних організаціях;
- враховувати основні положення політики інформаційної безпеки в інноваційних організаціях;
- використовувати основні функції служби захисту інформації інноваційної організації та особливості моніторингу системи інформаційної безпеки в інноваційних організаціях.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Основні поняття та визначення. Інноваційні процеси та їх класифікація. Стан сучасної кібербезпеки та шляхи розвитку на майбутнє. Конкурентні переваги при інноваційній діяльності.

Тема 2. Загрози та ризики витоку конфіденційної інформації. Аналіз проблеми оперативного виявлення і реагування на інциденти кібербезпеки в телекомунікаціях.

Тема 3. Сучасні тенденції в галузі захисту інформації інноваційного підприємництва. Комерційна інформація та комерційна таємниця.

Тема 4. Структура і завдання політики інформаційної безпеки. Кадрова політика, моніторинг і контроль. Захист від недоброчесної конкуренції та шпигунства. Створення та впровадження програми навчання працівників у сфері кібербезпеки (SAT).

Тема 5. Соціальна інженерія. Загрози кіберсистемам. Використання методів соціальної інженерії для захисту інноваційної діяльності від кібератак.

Тема 6. Управління контролем доступу. Основна функція управління контролю доступом.

Тема 7. Перспективи систем забезпечення інформаційної безпеки кіберпростору. Кібербезпека комунікаційних систем і мереж.

Тема 8. Засоби захисту від витоку інформації в Інтернет. Програмно-апаратні системи шифрування, брандмауери, системи попередження вторгнення.

Тема 9. Протокол захисту електронних транзакцій TLS. Порівняння версій протоколів TLS 2.0 та 3.0.

Тема 10. Захист електронної пошти. Боротьба зі спамом та фішингом.

Тема 11. Безпека мережі з програмованими параметрами SDN.

Тема 12. Додаткові методи підвищення безпеки мережі ІКТ.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин							
	денна форма				Заочна форма			
	усього	у тому числі			усього	у тому числі		
		лекц.	практ.	сам. роб.		лекц	Практ.	сам.роб.
Тема 1 **Основні поняття та визначення.** Інноваційні процеси та їх класифікація. Стан сучасної кібербезпеки та шляхи розвитку на майбутнє. Конкурентні переваги при інноваційній діяльності.	10	2		8	10	2		8
Тема 2. **Загрози та ризики витоку конфіденційної інформації.** Загрози інформаційної безпеки держави в соціальних мережах. Аналіз проблеми оперативного виявлення і реагування на інциденти кібербезпеки в телекомунікаціях.	10	2	2	6	10		2	8
Тема 3. **Сучасні тенденції в галузі захисту інформації інноваційного підприємництва.** Комерційна інформація та комерційна таємниця.	10	2	2	6	10			10
Тема 4. **Структура і завдання політики інформаційної безпеки.** Кадрова політика, моніторинг і контроль. Захист від недоброчесної конкуренції та шпигунства. Створення та впровадження програми навчання працівників у сфері кібербезпеки (SAT).	10		2	8	10		2	8
Тема 5. **Соціальна інженерія**. Загрози кіберсистемам. Використання методів соціальної інженерії для захисту інноваційної діяльності від кібератак.	10	2	2	6	10			10
Тема 6. **Управління контролем доступу.** Основна функція управління контролю доступом.	10	2	2	6	10	2		8
Тема 7. **Перспективи систем забезпечення інформаційної безпеки кіберпростору**. Кібербезпека комунікаційних систем і	10	2	2	6	10			10

мереж.								
Тема 8. **Засоби захисту від витоку інформації в Інтернет.** Програмно-апаратні системи шифрування, брандмауери, системи попередження вторгнення.	10	2	2	6	10		2	8
Тема 9**. Протокол захисту електронних транзакцій TLS**. Порівняння версій протоколів TLS 2.0 та 3.0	10	2	2	6	10	2		8
Тема 10. **Захист електронної пошти.** Боротьба зі спамом та фішингом.	10	2	2	6	10			10
Тема 11. **Безпека мережі з програмованими параметрами SDN.**	10	2	2	6	10			10
Тема 12. **Додаткові методи підвищення безпеки мережі ІКТ.**	10	2	2	6	10			10
Усього годин	**120**	**22**	**22**	**76**	**120**	**6**	**6**	**108**
ПІДСУМКОВИЙ КОНТРОЛЬ – **залік**								

5. ПРАКТИЧНІ ЗАНЯТТЯ

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1	Аналіз методів стимулювання інноваційної діяльності [с. 26-32]	2	
2	Дослідження методів захисту інформації при інноваційній діяльності [с. 46-53]	4	2
3	Вивчення алгоритму формування систем інформаційної безпеки [с. 71-83]	2	
4	Дослідження основ теорії інформаційної безпеки [с. 95-101]	4	
5	Аналіз методів формування рейтингових систем інформаційної безпеки інноваційних процесів та підприємств [с. 102-113]	4	2
6	Дослідження алгоритму розробки показників надійності кібербезпеки [с. 160-177]	2	
7	Аналіз взаємодії видів безпеки в інноваціях на прикладі економічної безпеки [с. 33-41]	4	2
	Всього	22	6

7. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «**Інформаційна безпека інноваційної діяльності»** включаються наступні тематики завдання.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1.** Вивчення Положення закону «Про національну безпеку України»	8	8
2	**Тема 2.** Вивчення Положення закону України «Про інноваційну діяльність» .	6	8
3	**Тема 3.** Дослідження впливу витоку конфіденційної інформації на стан розвитку сучасного підприємсива.	6	10
4	**Тема 4.** Дослідження методів захисту від недоброчесної конкуренції та шпигунства**.** Дослідження програми навчання працівників у сфері кібербезпеки (SAT).	8	8
5	**Тема 5.** Класифікація кіберзагроз та види кібератак.	6	10
6	**Тема 6.** Дослідження мережевих систем виявлення вторгнень.	6	8
7	**Тема 7.** Дослідження комплексного підходу виявлення вторгнень заснований на аналізі трафіка.	6	10
8	**Тема 8.** Дослідження порівняльної характеристики сучасних криптосистем, що використовуються для захисту конфіденційної інформації**.**	6	8
9	**Тема 9.** Дослідження протоколу захисту електронних транзакцій 3D-Secur для додаткового кроку автентифікації**.**	6	8
10	**Тема 10.** Класифікація загроз та правила поведінки працівників в корпоративній мережі.	6	10
11	**Тема 11.** Дослідження Віртуальних спільнот, як суб'єктів інформаційної безпеки Держави.	6	10
12	**Тема 12.** Дослідження моделі забезпечення безпеки в комп'ютерних системах.	6	10
	Всього	**76**	**108**

8. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Робоча програма навчальної дисципліни передбачає наступні види та методи контролю:

Види контролю	Складові оцінювання
Поточний контроль, який здійснюється у ході: проведення практичних та лабораторних занять, виконання індивідуального завдання; проведення консультацій та відпрацювань.	50%
Підсумковий контроль, який здійснюється у ході проведення іспиту (заліку).	50%

Методи діагностики знань (контролю)	Фронтальне опитування, лабораторні завдання, індивідуальні завдання, робота у групах, розв`язання практичних завдань, залік

Питання до заліку

1. Що таке інформаційна безпека і які її основні складові?

2. Які основні загрози інформаційній безпеці існують?

3. Як класифікуються загрози інформаційній безпеці інноваційних проєктів?

4. Що таке конфіденційність інформації?

5. Що таке цілісність інформації?

6. Що таке доступність інформації?

7. Як поняття інформаційної безпеки застосовується до інноваційних продуктів?

8. Які нормативно-правові акти регулюють інформаційну безпеку в Україні?

9. Які міжнародні стандарти інформаційної безпеки є найбільш поширеними?

10. Що таке GDPR і як він впливає на інформаційну безпеку інноваційної діяльності?

11. Які вимоги до захисту персональних даних існують у рамках законодавства України?

12. Які етичні аспекти необхідно враховувати при забезпеченні інформаційної безпеки?

13. Які основні технічні засоби забезпечення інформаційної безпеки існують?

14. Що таке криптографія і яку роль вона відіграє в захисті інформації?

15. Які різновиди антивірусного програмного забезпечення існують?

16. Як застосовуються системи виявлення і попередження вторгнень у інноваційній діяльності?

17. Які сучасні технології застосовуються для забезпечення безпеки мережевих інноваційних систем?

18. Що таке політика інформаційної безпеки і як її формують?

19. Які основні складові політики інформаційної безпеки інноваційних компаній?

20. Як розробляється політика резервного копіювання інформації?

21. Які заходи потрібно вжити для захисту інформації під час інноваційного проєкту?

22. Що таке інцидент інформаційної безпеки і як з ним боротися?

23. Як забезпечити інформаційну безпеку на всіх етапах життєвого циклу інноваційного продукту?

24. Які особливості інформаційної безпеки у сфері стартапів?

25. Як здійснюється захист інформаційних активів інноваційних компаній?

26. Як нові технології (наприклад, блокчейн) можуть вплинути на інформаційну безпеку інноваційних проєктів?

27. Як захистити інтелектуальну власність у сфері інноваційної діяльності?

28. Яку роль відіграє людський фактор у забезпеченні інформаційної безпеки?

29. Які методи соціальної інженерії використовують для викрадення інформації?

30. Як можна підвищити обізнаність співробітників щодо загроз інформаційній безпеці?

31. Які засоби захисту від інсайдерських загроз застосовуються у компаніях?

32. Як проводити навчання працівників щодо політик інформаційної безпеки?

33. Які типи інформаційних атак існують?

34. Як відрізняються DDoS-атаки від інших мережевих атак?

35. Які методи використовуються для виявлення та запобігання фішинговим атакам?

36. Що таке атаки нульового дня і як з ними боротися?

37. Які заходи безпеки необхідно вжити для захисту інноваційного продукту від кібератак?

38. Які методи використовуються для захисту програмного забезпечення від несанкціонованого доступу?

39. Що таке уразливості програмного забезпечення і як їх можна уникнути?

40. Як забезпечити безпеку мобільних додатків у інноваційних проєктах?

41. Які сучасні виклики та тенденції в галузі інформаційної безпеки інновацій?

42. Як впливають технології штучного інтелекту на інформаційну безпеку?

43. Яку роль відіграє хмарне зберігання даних у забезпеченні інформаційної безпеки?

44. Як впливають великі дані (Big Data) на інформаційну безпеку інноваційних проєктів?

45. Які вимоги до захисту персональних даних існують у рамках законодавства України?

9. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ СТУДЕНТІВ (для заліку)

Рівень знань оцінюється:

– «відмінно» / «зараховано» A – від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях, практичних та лабораторних заняттях, під час яких виконував усі поставленні завдання та давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, виконав лабораторні роботи та завдання до самостійної роботи, проявляє активність і творчість у науково-дослідній роботі;

– «добре» / «зараховано» B – від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях, практичних та лабораторних заняттях, під час яких виконував усі поставленні завдання та давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, виконав лабораторні роботи та завдання до самостійної роботи, проявляє активність і творчість у науково-дослідній роботі;

– «добре» / «зараховано» C – від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність виконаних лабораторних робіт та завдань до самостійної роботи та активність у науково-дослідній роботі;

– «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та практичних заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність виконаних лабораторних робіт та завдань до самостійної роботи;

– «задовільно» / «зараховано» E – від 60 до 63 балів. Студент був присутній не на всіх лекціях та практичних заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, виконав не всі завдання до самостійної роботи;

– «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу;

– «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 1 до 34 балів. Студент не володіє навчальним матеріалом.

Таблиця відповідності результатів контролю знань за різними шкалами

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	Зараховано
74-81	C		
64-73	D	Задовільно	Зараховано
60-63	E		
35-59	Fx	Незадовільно	Не зараховано
1-34	F		

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1 . Кононович В.Г., Стайкуца С.В., Севастєєв Є.О., Швець О.В. Інформаційна безпека інноваційної діяльності в інфокомунікаціях : підручник та дистанційний практикум. За ред. д.т.н., проф. В.В.Корчинського. Післямова д.т.н., проф. С.О.Гнатюка. Одеса: ДУІТЗ, 2022. 298 с. (для аудиторного та дистанційного навчання, мова: укр., англ).

Допоміжна

2. Криптографічний захист інформації: Навч. посіб./Онацький О.В., Йона Л.Г., Бєлова Ю.В.. - Одеса: ДУІТЗ, 2023. – 250 с..

Інформаційні ресурси

1 Наказ МОН № 332 від 18.03.2021 року Про затвердження стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти. URL: https://osvita.ua/legislation/Vishya_osvita.
2 Національна бібліотека України ім. В.І. Вернадського. URL: http://www.nbuv.gov.ua.
3 Портал кіберполіції України. URL: https://cyberpolice.gov.ua/
4 Портал урядової команди реагування на комп’ютерні надзвичайні події України (CERT-UA). URL: https://cert.gov.ua/
5 Radivilova, L. Kirichenko, M. Tawalbeh, P. Zinchenko, V. Bulakh, «Балансування самоподібного трафіку в мережних системах виявлення вторгнень », Кібербезпека: освіта, наука, техніка, Том. 3, вип. 7, с. 17-30, Бер 2020. DOI: https://doi.org/10.28925/2663-4023.2020.7.1730 (Радівілова, Л. Кириченко, М. Тавалбе, П. Зінченко, В. Булах, «Балансування самоподібного трафіку в мережевих системах виявлення вторгнень», Кібербезпека: освіта, наука, техніка, Том. 3, вип. 7, с. 17-30, Бер 2020. DOI: https://doi.org/10.28925/2663-4023.2020.7.1730)
6 4. Радівілова Т.А., Ільков А.А., Тавалбех М.Х. Комплексний метод виявлення вторгнень заснований на статистичному та динамічному підходах аналізу трафіка. Радиоэлектроника и информатика. № 01. 2020. С. С.17-25.
7 Комплекс навчально-методичного забезпечення навчальної дисципліни "Захист систем електронної комерції та мультисервісних систем", освітньо-кваліфікаційний рівень бакалавр для спеціальності 125 - Кібербезпека [Електронний ресурс] : освітня програма підготовки "Управління інформаційною безпекою" / ХНУРЕ ; розроб. Т.А. Радівілова. – Харків, 2019. – 397 с. - pdf / 13,03 Mb.