ЗАТВЕРДЖЕНО

Вченою радою
факультету інформаційно-
комп'ютерних технологій
31 серпня 2023 р., протокол № 5

Голова Вченої ради
_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 10 «ПРОЕКТУВАННЯ СИСТЕМ КІБЕРБЕЗПЕКИ»

для здобувачів вищої освіти освітнього ступеня «магістр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної інженерії та
кібербезпеки
28 серпня 2023 р., протокол № 7

Завідувач кафедри
_____ Андрій ЄФІМЕНКО

Гарант освітньо-
професійної програми
_____ Володимир ВОРОТНІКОВ

Розробник: кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення Надія ЛОБАНЧИКОВА, доктор технічних наук, доцент, професор кафедри комп'ютерної інженерії та кібербезпеки Володимир ВОРОТНІКОВ

Житомир
2023 – 2024 н.р.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів –4</td><td>Галузь знань
12 «Інформаційні технології»</td><td colspan="2">Обов’язкова компонента ОП</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність
125 «Кібербезпеки та захист інформації»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 4</td><td>1-й</td><td>-</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 120</td><td>2-й</td><td>-</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="12">Тижневих годин для денної форми навчання:
аудиторних 4
самостійної роботи – 5,4</td><td rowspan="12">Освітній ступінь «Магістр»</td><td>32 год.</td><td>-.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>год.</td><td>-</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32 год.</td><td>-.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>56 год.</td><td>-</td></tr>
<tr><td colspan="2">Індивідуальне завдання:
курсова робота</td></tr>
<tr><td>–</td><td></td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td colspan="2">екзамен</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи;

для заочної форми навчання − 10% аудиторних занять, 90 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є ознайомлення студентів з сутністю, задачами, принципами та сучасними технологіями проектування систем кібербезпеки для комплексного захисту інформації; методологічними та законодавчими основами організації, планування, проектування, впровадження, експлуатації та супроводу систем кібербезпеки; основним аспектам практичної діяльності по їх проектуванню, розробці, реалізації та забезпеченню функціонування; проведення оцінки ефективності з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників; освоєння сучасних комп'ютерних технологій проектування систем захисту інформації з використанням графічних програмних середовищ візуального моделювання UML і особливостей проектування систем за допомогою CASE-засобів.

Завданнями вивчення навчальної дисципліни є:

Зн1. Формування спеціалізованих концептуальних знань, що включають сучасні наукові здобутки у сфері професійної діяльності та інформаційних технологій і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем кібербезпеки та інформаційних технологій загалом;

Ум1 Для формування спеціалізованих умінь/навичок розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур:

– оволодіння етапами проектування систем кіберзахисту;

– розуміння головних задач та сервісів кібербезпеки;

– оволодіння методологічними та законодавчими основами організації, планування, проектування, впровадження, експлуатації та супроводу систем кібербезпеки;

Ум2 Для формування здатності інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах:

– вивчення основних принципів, засад та методів організаційного та технічного проектування систем захисту в кіберпросторі;

– оволодіння методами та технологіями розробки супроводжувальної робочої документації;

– оволодіння методами оцінки ефективності систем кіберзахисту;

Ум3. Для формування здатності розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності:

– освоєння сучасних комп'ютерних технологій проектування систем захисту інформації з використанням графічних програмних середовищ візуального моделювання UML і особливостей проектування систем за допомогою CASE-засобів.

Зміст освітньої компоненти направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації»:

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

КЗ-2. Здатність проводити дослідження на відповідному рівні.

КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КФ-1. 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.

КФ-2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

КФ-3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

КФ-4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 125 «Кібербезпека та захист інформації»:

РН-2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН-3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН-4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН-5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання

спеціалізованого програмного забезпечення.

РН-6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН-7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН-8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

РН-12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

РН-13. 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.

РН-15. 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..

РН-16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

РН-19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН-20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН-21. . Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН-22. 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.

РН-23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Досягнення Комунікації **К1** здійснюється за рахунок захисту звітів з лабораторних робіт та відкритого захисту курсової роботи з освітньої компоненти. Досягнення відповідальності та автономії досягається за рахунок виконання курсової роботи та виконання індивідуальних завдань в межах лабораторних робіт.

3. Програма навчальної дисципліни

Змістовий модуль 1. Теоретичні аспекти проектування систем кібербезпеки

Тема 1. Термінологія. Нормативно-правове регулювання

Понятійний апарат. Проекти: принципи, стадії та етапи створення. Управління проектами розробки та впровадження систем кібербезпеки. Класифікація проектів.

Тема 2. Методи планування та оцінки систем кібербезпеки

Структурне планування. Календарне планування. Оцінка якості та економічної ефективності систем кібербезпеки. Стандарти керування якістю промислової продукції.

Тема 3. Життєвий цикл систем захисту інформації

Основні, допоміжні та організаційні процеси життєвого циклу СЗІ. Структура життєвого циклу СЗІ. Моделі життєвого циклу СЗІ.

Тема 4. Проектна документація. Колективна робота над проектами.

Типова технічна документація. Особливості оформлення, технічні аспекти. Документи супроводу та введення в експлуатацію систем.

Соціальні та морально етичні норми колективного розроблення проектів. Оптимізація та сучасні інформаційні технології розробки проектів. Огляд Agile-методологія. Scram-framework. Kanban, XP.

Змістовий модуль 2 Концептуальні положення проектування та моделювання систем захисту інформації

Тема 5. Основні концептуальні положення побудови систем захисту інформації

Концептуальні підходи до проектування систем захисту інформації. Комплекс інженерно-технічного захисту інформації. Приклад багаторівневої

інтегрованої автоматизованої системи охорони особливо важливих об'єктів. Особливості побудови систем захисту від несанкціонованого доступу.

Тема 6. Процедури системного проектування та моделювання.

Ітераційна процедура системного проектування. Модель автоматизованої системи виявлення та попередження НС. Модель прояву суб'єктів погроз виникнення НС.

Тема 7. Методологія проектування систем захисту інформації

Прикладний аспект: модель процесу виявлення та попередження НС у зоні загального доступу території аеропорту; метод визначення рівня небезпеки суб'єктів погроз виникнення НС; модель процесу виявлення та попередження НС в контрольованих зонах території аеропорту.

Тема 8. Загальні положення та визначення об'єктно-орієнтованого моделювання і проектування.

Основи методології проектування систем захисту інформації. Методологія процедурно-орієнтованого програмування. Методологія об'єктно-орієнтованого аналізу і програмування. Методологія системного аналізу і системного моделювання. Розвиток методології об'єктно-орієнтованого аналізу і проектування систем.

Змістовий модуль 3. Методологія та технології розробки систем кібербезпеки

Тема 9. Процесний та імітаційні підходи у проектуванні.

Методи IDEF. Принципи побудови моделі IDEF0. Діаграми IDEF0: контексна діаграма, діаграма декомпозиції, діаграма дерева вузлів, діаграма тільки для експозиції. Робота функції (Activity). Стрілки(Arrow) та зв'язки.

Методологія структурного аналізу SA (Structured Analysis). Методологія структурного проектування SD (Structured Design). Структурно-системний аналіз SSA (Structured Systems Analysis). Структурного системний аналіз і проектування SA/SD. Методології SRD (Structured Requirements Definition), SSADM (Structured Systems Analysis and Design Method). Діаграми потоків даних- DFD.

Тема 10. Діаграми концептуального, логічного і фізичного моделювання UML

Проектування та моделювання систем захисту інформації за допомогою UML. Призначення та загальна структура мови моделювання UML. Основні пакети та опис метамоделі UML. Відношення у мові моделювання UML та позначення цих відношень.

Діаграми варіантів використання (use case diagram) системи: основні елементи діаграми; відношення на діаграмі елементів використання; текстові сценарії елементів використання; рекомендації для розроблення діаграм варіантів використання. Приклад побудови діаграми. Діаграми класів (class diagram) системи: класи та відношення між ними; розширення UML для

побудови моделей програмного забезпечення; шаблони або параметризовані класи; моделювання та проектування класів. Приклад побудови діаграми. Діаграми кооперації (collaboration diagram) системи: основні елементи діаграми; відношення на діаграмі та зв'язки; рекомендації щодо побудови діаграми кооперації. Приклад побудови діаграми. Діаграми послідовності (sequence diagram) дій системи: основні елементи діаграми; відношення на діаграмі та зв'язки; примітки; рекомендації щодо побудови діаграми послідовності дій. Приклад побудови діаграми. Діаграми станів системи (statechart diagram): основні елементи діаграми; відношення на діаграмі та зв'язки; рекомендації щодо побудови діаграми станів. Приклад побудови діаграми. Діаграми діяльності (активності) (activity diagram) системи: основні елементи діаграми; відношення на діаграмі та зв'язки; рекомендації щодо побудови діаграми діяльності; переходи; доріжки; об'єкти. Приклад побудови діаграми. Діаграми компонентів (component diagram) та діаграми розгортання: компоненти; інтерфейси; залежності; вузли; з'єднання і залежності. Приклади побудови діаграм компонентів і діаграм розгортання.

Змістовий модуль 4. Реалізація проекту систем кібербезпеки

Тема 11. Розробка програми та методики випробування. Реалізація проекту.

Документація. Особливості проведення. Адаптація до вимог стандартів.

Організація робіт із створення, виготовлення, монтажу, налагодження, випробування і здавання в експлуатацію систем і засобів забезпечення кібербезпеки. Документація.

Тема 12. Кваліфікаційний аналіз засобів та систем захисту інформації

Загальні вимоги до кваліфікаційного аналізу. Організація державної експертизи. Розроблення комплектів керівних документів щодо забезпечення робіт з удосконалення, модернізації, уніфікації систем, засобів і технологій забезпечення кібербезпеки. Документація.

Тема 13. Оцінка ефективності систем захисту інформації.

Підходи до оцінки ефективності систем захисту інформації.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	лабораторні	Самостійна робота	усього	лекції	практичні	Самостійна робота
Модуль 1								
Змістовий модуль 1. Теоретичні аспекти проектування систем кібербезпеки								
Тема 1. Термінологія. Нормативно-правове регулювання	6	2		4				
Тема 2. Методи планування та оцінки систем кібербезпеки	8	2	2	4				
Тема 3. Життєвий цикл систем захисту інформації	8	2	2	4				
Тема 4. Проектна документація. Колективна робота над проектами.	8	2	2	4				
Разом за змістовий модуль 1	30	8	6	16				
Змістовий модуль 2. Концептуальні положення проектування та моделювання систем захисту інформації								
Тема 5. Основні концептуальні положення побудови систем захисту інформації	6	2	2	2				
Тема 6. Процедури системного проектування та моделювання.	6	2	2	2				
Тема 7. Методологія проектування систем захисту інформації	6	2	2	2				
Тема 8. Загальні положення та визначення об’єктно-орієнтованого моделювання і проектування.	8	2	2	4				
Разом за змістовий модуль 2	30	8	8	10				
Змістовий модуль 3. Методологія та технології розробки систем кібербезпеки								
Тема 9. Процесний та імітаційні підходи у проектуванні	10	2	4	4				
Тема 10. Діаграми концептуального, логічного і фізичного моделювання UML	26	6	10	10				
Разом за змістовий модуль 3	36	8	14	14				
Змістовий модуль 4. Реалізація проекту систем кібербезпеки								
Тема 11. Розробка програми та методики випробування. Реалізація проекту.	6	2		4				
Тема 12. Кваліфікаційний аналіз засобів та систем захисту інформації	8	2	2	4				
Тема 13. Оцінка ефективності систем захисту інформації.	14	4	2	8				
Разом за змістовий модуль 4	28	8	4	16				
ВСЬОГО	120	32	32	56				

5. Теми лабораторних робіт

№ З/П	НАЗВА ТЕМИ	КІЛЬКІСТЬ ГОДИН	
		ДЕННА ФОРМА	ЗАОЧНА ФОРМА
1	Дослідження процесів побудови системи захисту інформації режимно-секретного органу	2	
2	Дослідження процесів мережевого планування і управління проектами розробки і впровадження систем	2	
3	Дослідження процесів розробки технічного завдання на створення комплексної системи захисту інформаційних ресурсів від несанкціонованого доступу	2	
4	Дослідження структури запропонованої СЗІ, побудова моделі взаємодії компонентів системи	4	
5	Дослідження процесів побудови функціональних моделей системи	4	
6	Дослідження процесів побудови моделей бази даних	4	
7	Дослідження процесів побудови UML діаграм	4	
8	Дослідження процесів побудови діаграми класів	4	
9	Дослідження процесів побудови діаграми послідовності дій	2	
10	Дослідження процедур оцінки комплексних систем захисту інформації	4	
РАЗОМ		32	

6. Завдання для самостійної роботи

Тема 1. Термінологія. Нормативно-правове регулювання

Самостійна робота за темою:

- опрацювання нормативно-правового забезпечення дисципліни;
- вивчення основних понять та визначень;
- порядок проведення робіт із створення СЗІ.

Рекомендована література 1-28, 30, 35, 51, 54, 61

Тема 2. Методи планування та оцінки систем кібербезпеки.

Самостійна робота за темою:

- функціональні методи оцінки ризиків;
- процес загального оцінювання ризику;
- аналізування небезпечних чинників і критичні точки контролю.

Рекомендована література 27-32, 35, 43-44, 52, 56, 58.

Тема 3. Життєвий цикл систем захисту інформації

Самостійна робота за темою:

- основні фази проектування;
- основні, допоміжні та організаційні процеси життєвого циклу систем захисту інформації;
- структура життєвого циклу систем захисту інформації;
- моделі життєвого циклу систем захисту інформації.

Рекомендована література: 2, 8, 17, 22, 30, 38, 43, 56, 61.

Тема 4. Проектна документація. Колективна робота над проектами

Самостійна робота за темою:

– основі складові, порядок розроблення, зміст, вимоги до змісту технічного завдання;

– вимоги до системи захисту інформації та складу проектної та експлуатаційної документації;

– специфіка, моделі та методи побудови систем захисту режимних об’єктів

Рекомендована література 2, 8, 17, 22, 30, 38, 43, 56, 61.

Тема 5. Основні концептуальні положення побудови систем захисту інформації

Самостійна робота за темою:

- концептуальні підходи до проектування систем захисту інформації;
- комплекс інженерно-технічного захисту інформації;

– приклад багаторівневої інтегрованої автоматизованої системи охорони особливо важливих об’єктів;

– особливості побудови систем захисту від несанкціонованого доступу

Рекомендована література 8-9, 19, 22-26, 28-36, 39-47, 52-58.

Тема 6. Процедури системного проектування та моделювання.

Самостійна робота за темою:

– методологія системного аналізу і системного моделювання;

– розвиток методології об’єктно-орієнтованого аналізу і проектування систем;

– методологія процедурно-орієнтованого програмування;

– методологія об’єктно-орієнтованого аналізу і програмування.

Рекомендована література 8-9, 19, 22-26, 28-36, 39-47, 52-58.

Тема 7. Методологія проектування систем захисту інформації

Самостійна робота за темою:

– загальна методологія побудови системи захисту інформації (СЗІ) типового об’єкту;

– основні складові СЗІ та їх внесок в вирішення проблеми інформаційної безпеки;

– сутність комплексного (інтегрального) підходу до захисту інформації;

– призначення та функції основних підсистем у складі типової СЗІ.

Рекомендована література 8-9, 19, 22-26, 28-36, 39-47, 52-61.

Тема 8. Загальні положення та визначення об’єктно-орієнтованого моделювання і проектування.

Самостійна робота за темою:

– **-** Методи структурного аналізу і проектування ПЗ;

– – Методи об'єктно орієнтованого аналізу і проектування ПЗ;

– Об'єктно-орієнтоване проектування архітектури GUI.

Рекомендована література 8-10, 16, 22, 25, 38, 40, 58.

Тема 9. Процесний та імітаційні підходи у проектуванні

Самостійна робота за темою:

– еволюція процесних уявлень регламентації;

– процесний підхід до управлінських рішень, поняття проблеми, проблемної ситуації, процесу прийняття рішення;

– процесний, системний і ситуаційний підходи в управлінні.

Рекомендована література 7-8, 26-30, 33, 34, 36, 39, 40, 43.

Тема 10. Діаграми концептуального, логічного і фізичного моделювання UML

Самостійна робота за темою:

– діаграми діяльності (активності) (activity diagram) системи;
– діаграми компонентів (component diagram);
– діаграми розгортання;
– технологій розробки систем захисту інформації.

Рекомендована література 30-31, 54-57.

Тема 11. Розробка програми та методики випробування. Реалізація проекту

Самостійна робота за темою:

– розробка і реалізація програми (бізнес-проекту) трансформації підприємств;
– управління IT-проектами

Рекомендована література 24, 25, 28, 31, 37- 40, 43-44.

Тема 12. Кваліфікаційний аналіз засобів та систем захисту інформації

Самостійна робота за темою:

– моделювання комплексних систем захисту інформації;
– спеціальні методи неформального моделювання;
– розробка програм і проектів нововведень.

Рекомендована література 8, 22, 27, 30, 31, 39, 43, 44, 52, 54, 60.

Тема 13. Оцінка ефективності систем захисту інформації

Самостійна робота за темою

– програма оцінки ефективності систем захисту інформації "Оцінка СЗІ";
– оцінка ефективності комплексної системи захисту інформації в системі оперативного інформування МВС України;
– проблеми оцінки ефективності систем захисту.

Рекомендована література 8, 22, 27, 30, 31, 39, 43, 44, 52, 54, 60.

Виконання самостійної роботи студентів можливе у вигляді проходження зазначеного викладачем курсу Cisco. Здача фінального тесту з вказаного курсу переводиться в бали, виділені для самостійної роботи та заноситься до рейтингу поточного оцінювання студента.

Вимоги до оформлення звітів з самостійної роботи студентів:

Звіт з самостійної роботи студентів оформлюється на аркушах формату А4 (210х297 мм) на одній стороні листа білого паперу у вигляді: титульний аркуш, теоретичні питання, список використаної літератури.

Звіт виконується в електронному варіанті (система Windows, текстовий процесор Word) *Вимоги до тексту*: заголовок – 16 пт, текст відповіді – 14 пт, вирівняти по ширині, абзаци зі стандартним відступом першого рядка, інтервал міжрядковий – 1,5, поля: ліве – 3 см, праве – 1 см, верхнє, нижнє – 2 см, колонтитули із зазначенням ПІБ, номера сторінки. Об'єм звіту з самостійної роботи по темі складає 4-7 сторінки.

Якість роботи оцінюється з урахуванням правильності відповідей, підбору літератури, проведеного аналізу та відповідність звіту вказаним вимогам щодо оформлення. Захист звітів (рефератів) з самостійної роботи відбувається шляхом опитування на лабораторній роботі або консультації та представлення презентації реферату.

Критерії оцінювання знань та вмінь студента за результати виконання самостійної роботи за національною шкалою

За результати виконання самостійної роботи студенту виставляється оцінка:

в і д м і н н о, якщо студент вміє використовувати основну та додаткову літературу, в письмовій доповіді повністю і якісно розкрив тему, методично обґрунтовано використав теоретичні знання та практичні навички, у висновках дав вірну технічну інтерпретацію, грамотно оформлену роботу подав в установлений термін, доповідь студента чітка, грамотна, супроводжується комп'ютерною презентацією. Студент вірно та обґрунтовано відповів на поставлені питання з наведенням прикладів та аргументуванням своєї власної точки зору. Допускається наявність незначної кількості огріхів та несуттєвих неточностей, які не призвели до помилок у відповіді;

д о б р е, якщо студент вміє використовувати основну та додаткову літературу, в письмовій доповіді повністю і якісно розкрив тему, методично обґрунтовано використав теоретичні знання для виконання завдань, у висновках дав вірну технічну інтерпретацію, допустив несуттєву помилку у відповіді або висновках, допустив незначні відхилення від чинних стандартів при оформленні роботи;

з а д о в і л ь н о, якщо студент в письмовій доповіді розкрив тему, але виконану роботу подав більше двох тижнів після встановленого терміну, допустив помилки у відповіді або висновках, оформлення роботи, не зовсім відповідає чинним вимогам стандартів, доповідь не супроводжується комп'ютерною презентацією.

н е з а д о в і л ь н о, якщо студент в письмовій доповіді не розкрив тему, не виконав завдання, отримані результати у висновках інтерпретуються невірно, робота оформлена неохайно.

Критерії переводу балів за результати виконання самостійної роботи з національної шкали в бали ECTS

Відповідність балів національної і кредитно-модульної шкали за виконання самостійної роботи:

Оцінка виконаної студентом самостійної роботи за національною шкалою	Бали ECTS	Оцінка ECTS
5	13,5...15,0	A
4	12,3...13,4	B
	11,1…12,2	C
3	9,6...11,0	D
	9,0...9,5	E
2	5,3…8,9	F
	<5,3	FX

7. Індивідуальні завдання

Виконання індивідуального завдання (ІЗ) є важливою частиною дисципліни «Проектування систем кібербезпеки» та представляє собою самостійне дослідження студента, яке представляється у вигляді виконання курсової роботи.

Мета виконання ІЗ є закріплення, узагальнення та поглиблення знань, одержаних студентами під час вивчення дисципліни та їх застосування при самосійній роботі, активізація творчих здібностей студентів, розвиток навичок роботи з нормативно-технічною літературою, прийняття самостійних рішень, набуття практичних навичок роботи щодо захисту інформації програмними та криптографічними засобами.

ІЗ повинно бути результатом самостійних досліджень студента, які:

– сприяють розвитку ініціативності студентів у їх виробничій і дослідницькій діяльності;

– поглиблюють, систематизують та закріплюють теоретичні знання та практичні навички, отримані під час навчання;

– перевіряють уміння студента самостійно освоювати та використовувати сучасні інформаційні технології;

– розвивають у студента навички ведення самостійного науково-практичного пошуку, оволодіння методикою дослідження й експериментування в ході вирішення проблем і питань, поставлених до виконання;

– сприяють набуттю вміння аналізувати отримані результати досліджень, формулювати висновки та положення.

За всі відомості, що викладені в ІЗ, порядок використання в ході підготовки фактичного матеріалу та іншої інформації, пропозиції, технології, обґрунтованість і вірогідність висновків та положень, що захищаються, несе відповідальність безпосередньо автор.

Викладач надає студенту допомогу у виборі теми роботи, проводить консультації з проблемних питань, що виникають у процесі виконання, надає допомогу в пошуку методичної та технічної документації, науково-технічної літератури.

Виконання курсової роботи здійснюється відповідно до методичних рекомендацій: Методичні рекомендації для виконання курсової роботи з навчальної дисципліни «Проектування систем кібербезпеки» для здобувачів вищої освіти освітнього ступеня «магістр» спеціальності 125 «Кібербезпека» (автори: Лобанчикова Н.М., Ющенко О.О.), 2022. 48 с. Електронне видання (Протокол НМР №11 від 25.07.2022) - Режим доступу:http://surl.li/cqxcx

8. Методи навчання

На лекційних заняттях: розповідь, пояснення, демонстрація, бесіда, дискусія. На лабораторних роботах: пояснення, дослідження, розв`язування ситуаційних задач, виконання індивідуального варіанту завдання. Самостійна робота студента: реферати, повідомлення, науково-пошукові, дослідницькі проекти, виконання он-лайн курсів.

За джерелами знань використовуються такі методи навчання: словесні – розповідь, пояснення, лекція, інструктаж; наочні – демонстрація, ілюстрація; практичні – лабораторна робота, практична робота, вправи. За характером логіки пізнання використовуються такі методи: аналітичний, синтетичний, аналітико-синтетичний, індуктивний, дедуктивний. За рівнем самостійної розумової діяльності використовуються методи: проблемний, частково-пошуковий, дослідницький.

9. Методи контролю

Контрольні заходи включають поточний та підсумковий модульний контроль в тому числі у вигляді комп’ютерних тестів, виконання лабораторних робіт.

Поточний контроль здійснюється під час проведення лабораторних занять для перевірки рівня підготовки студента до виконання конкретного завдання. Форма проведення поточного контролю: усне опитування, вирішення ситуаційних задач, тестовий контроль, комп’ютерне тестування, виконання практичного завдання. Оцінюється вхідний, проміжний, кінцевий рівень знань студента.

Підсумковий контроль проводиться у вигляді комп'ютерних тестів.

10. Розподіл балів

<table>
<tr><td colspan="4">Поточне оцінювання та самостійна робота</td><td>Сума</td></tr>
<tr><td colspan="4">Змістовий модуль 1 -26 балів</td><td rowspan="12">100</td></tr>
<tr><td>Т1</td><td>Т2</td><td>Т3</td><td>Т4</td></tr>
<tr><td>5</td><td>7</td><td>7</td><td>7</td></tr>
<tr><td colspan="4">Змістовий модуль 2- 22 бали</td></tr>
<tr><td>Т5</td><td>Т6</td><td>Т7</td><td>Т8</td></tr>
<tr><td>5</td><td>5</td><td>5</td><td>7</td></tr>
<tr><td colspan="4">Змістовий модуль 3 – 29 балів</td></tr>
<tr><td colspan="2">Т9</td><td colspan="2">Т10</td></tr>
<tr><td colspan="2">8</td><td colspan="2">21</td></tr>
<tr><td colspan="4">Змістовий модуль 4 – 21 бал</td></tr>
<tr><td colspan="2">Т11</td><td>Т12</td><td>Т13</td></tr>
<tr><td colspan="2">5</td><td>7</td><td>11</td></tr>
</table>

В межах ОК на освітньому порталі розміщено рейтинг лист, де детально можна ознайомитись з балами по кожному виду занять, поточному та підсумковому контролю.

Шкала оцінювання

За шкалою	Екзамен	Залік	Бали
A	Відмінно	Зараховано	90-100
B	Добре	Зараховано	82-89
C			74-81
D	Задовільно	Зараховано	64-73
E			60-63
FX	Незадовільно	Не зараховано	35-59
F		Не зараховано	0-34

11. Рекомендована література

Основна література

1. Конституція України. Режим доступу: https://zakon.rada.gov.ua/go/254к/96-вр
2. Закон України «Про захист інформації в інформаційно-комунікаційних системах», від 05.07.1994 № 81/94-ВР (Зі змінами, внесеними згідно із Законом № 1089-IX від 16.12.2020. Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
3. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
4. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
5. ISO/IEC 15408-1:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.
6. ISO/IEC 15408-2:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.
7. ISO/IEC 15408-3:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.
8. Інформаційні технології. Процеси життєвого циклу програмного забезпечення (ISO/IEC 12207:1995): ДСТУ 3918–1999. – [Чинний від 2000–01–01]. – К.: Держстандарт України, 2000. – 50 с. – (Національний стандарт України).
9. ISO/IEC 27002:2022 (en). Information security, cybersecurity and privacy protection – Information security controls// Online Browsing Platform (OBP). URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en
10. НД ТЗІ 1.1-002-99: Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
11. НД ТЗІ 2.5-004-99: Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
12. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
13. НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000, № 53.
14. Закон України «Про інформацію» № 2657-XИ від 02.10.1992. - ВВР, 1992, № 48, ст. 650.

15. Закон України «Про державну таємницю» № 3855-ХП від 21.01.1994, ВВР, 1994, № 16, ст. 93 (остання редакція № 1519-IV від 19.02.2004).

16. Закон України «Про електронні документи і електронний документообіг», № 851-IV від 22.05.2003, ВВР, 2003, № 36, ст. 275 (зі змінами, внесеними згідно із Законом № 2599-IV від 31.05.2005, ВВР, 2005, № 26, ст. 349).

17. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

18. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

19. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

20. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

21. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.

22. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.

23. ДБН 2.2-3-2004 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.

24. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.

25. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

26. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ-95). Затверджені наказом ДСТЗІ від 09.06.1995 № 25.

27. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

28. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія /Р.В. Грищук, Ю.Г. Даник; за заг. ред. проф. Ю.Г. Даника. Житомир : ЖНАЕУ, 2016 – 636 с.

29. Kevin Mitnick. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big./ Kevin Mitnick.– New York, Boston, London: Little, Brown and Company, 2017 – 320 с.

30. Лобанчикова Н.М. Захист інформації в АСУ: навч. посібник [Текст] / І. А. Пількевич, К. В. Молодецька, Н. М. Лобанчикова. – Житомир : Вид-во ЖДУ ім. І. Франка, 2014. – 170 с.

31. Лобанчикова Н.М. Основи побудови автоматизованих систем управління : навч. посібник [Текст] / І. А. Пількевич, К. В. Молодецька, І. І. Сугоняк, Н. М. Лобанчикова. – Житомир : Вид-во ЖДУ ім. І. Франка, 2014. – 174 с.

32. Lobanchykova, N.M., Pilkevych, I.A., Korchenko, O. Analysis of attacks on components of IoT systems and cybersecurity technologies. // Joint Proceedings of the Workshops on Quantum Information Technologies and Edge Computing (QuaInT+doors 2021), Zhytomyr, Ukraine, April 11, 2021. Edited by Serhiy O. Semerikov. (CEUR-WS.org). Pp. 83-96. http://ceur-ws.org/Vol-2850/paper6.pdf

33. Ihor Pilkevych, Oleg Boychenko, Nadiia Lobanchykova, Tetiana Vakaliuk, Serhiy Semerikov. Method of Assessing the Influence of Personnel Competence on Institutional Information Security // Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS, CEUR Workshop Proceedings, Khmelnytskyi, Ukraine, March 24–26, 2021. Edited by Tetiana Hovorushchenko, Oleg Savenko, Peter Popov, Sergii Lysenko. Pp. 266-275. http://ceur-ws.org/Vol-2853/paper33.pdf

34. N Lobanchykova, S Kredentsar, I Pilkevych and M Medvediev. Information technology for mobile perimeter security systems creation// Journal of Physics: Conference Series, Volume 1840, 012051, XII International Conference on Mathematics, Science and Technology Education (ICon-MaSTEd 2020) 15-17 October 2020, Kryvyi Rih, Ukraine. DOI: 10.1088/1742- 6596/1840/1/012022.

35. Лобанчикова Н.М. Модель побудови мобільної систем охорони периметру території .Сучасний захист інформації, 2020.Вип №1(41). С.42 – 48.

36. Матвійко А.В. Управління ІТ-проектами. – Львів: Новий світ-200, 2017. – 550 с.

37. Проектування, введення в дію та супроводження КСЗІ: навчальний посібник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, С.В. Зайцев. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 240 с.

38. Joseph Menn. Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World/ Joseph Menn.– New York: PublicAffairs, 2019.– 270.

39. Kevin Mitnick. Ghost In The Wires: My Adventures as the World's Most Wanted Hacker/ Kevin Mitnick.– New York, Boston, London: Little, Brown and Company, Back Bay Books, 2012 – 448 с.

Допоміжна література

40. Грайворонський М.В. Безпека інформаційно-комунікаційних систем/ М.В. Грайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009.– 608с.

41. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с. Режим доступу: Комплексні системи захисту інформації /

Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. / 2017 (vntu.edu.ua)

42. Akhmetov, B., Lakhno, V. (2018). System of decision support in weaklyformalized problems of transport cybersecurity ensuring, Journal of Theoretical and Applied Information Technology, 96 (8), pp. 2184-2196.

43. Akhmetov, B., Lakhno, V., Boiko, Y., Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity, Eastern-European Journal of Enterprise Technologies, 1 (2-85), pp. 4-15.

44. Akhmetov, B., Lakhno, V., Malyukov, V., Sarsimbayeva, S., Zhumadilova, M., Kartbayev, T. (2019). Decision support system about investments in smart city in conditions of incomplete information, International Journal of Civil Engineering and Technology, 10 (2), pp. 661-670/

12. Інформаційні ресурси в Інтернеті

51. Стандарти інформаційної безпеки: http://www.is-standard.com

52. Інформаційна безпеки: науковий журнал: http://www.nbuv.gov.ua/portal/natural/Ibez/index.html

54. Центр інформаційної безпеки: http://www.bezpeka.com

56. Журнал «Інформаційні технології. Аналітичні матеріали»: http://it.ridne.net/taxonomy/term/14