КАФЕДРА ЦИФРОВОЇ ЕКОНОМІКИ ТА БІЗНЕС-АНАЛІТИКИ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

ФАКУЛЬТЕТ УПРАВЛІННЯ ФІНАНСАМИ ТА БІЗНЕСУ

ЗАТВЕРДЖЕНО
на засіданні кафедри цифрової економіки та бізнес-аналітики
протокол № 6 від "21" січня 2020 р.

Зав. кафедри _____ Шевчук І.Б.
(підпис)

ЗАВДАННЯ ДЛЯ ІНДИВІДУАЛЬНОЇ РОБОТИ СТУДЕНТА (ІНДИВІДУАЛЬНІ НАВЧАЛЬНО-ДОСЛІДНІ ЗАВДАННЯ) І МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ЇХ ВИКОНАННЯ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в інформаційних системах
(назва навчальної дисципліни)

галузь знань: 05 «Соціальні та поведінкові науки»
(шифр та найменування галузі знань)

спеціальність: 051 "Економіка"
(код та найменування спеціальності)

спеціалізація: Інформаційні технології в бізнесі
(найменування спеціалізації)

освітній ступінь: бакалавр
(бакалавр/магістр)

Укладач:

Задорожна А. В., доцент, к.ф.-м.н., доцент
(ПІБ, посада, науковий ступінь, вчене звання)

ЛЬВІВ 2020

1. ЗАГАЛЬНІ МЕТОДИЧНІ РЕКОМЕНДАЦІЇ З ВИКОНАННЯ ІНДИВІДУАЛЬНИХ НАВЧАЛЬНО-ДОСЛІДНИХ ЗАВДАНЬ

Творча (евристична), наближена до наукового осмислення і узагальнення робота можлива лише як результат організації самостійного навчання з обов'язковою присутністю в ній цілепокладання та його досягнення за допомогою ефективних технологічних схем самоосвіти. Крім того, така робота повинна бути індивідуалізованою з врахуванням рівня творчих можливостей студента, його навчальних здобутків, інтересів, навчальної активності тощо.

Практична реалізація такого принципу навчання пов'язана із використанням в навчальному процесі індивідуальних навчально-дослідних завдань.

Індивідуальне навчально-дослідне завдання (ІНДЗ) є видом позааудиторної самостійної роботи студента навчального, навчально-дослідницького чи проектно-конструкторського характеру, яке використовується в процесі вивчення програмного матеріалу навчальної дисципліни і завершується разом із складанням чи заліку із даної навчальної дисципліни.

Метою ІНДЗ є самостійне вивчення частини програмного матеріалу, систематизація, поглиблення, узагальнення, закріплення та практичне застосування знань студента з навчальної дисципліни "Захист інформації в інформаційних системах" та розвиток навичок самостійної роботи.

Індивідуальні завдання повинні формувати уміння студентів самостійно працювати над рекомендованим матеріалом, висловлювати і захищати власну точку зору, орієнтувати студентів на засвоєння та закріплення головного, суттєвого при вивченні тем програми, розвивати самостійне мислення, навички розумової праці та вміння використовувати отримані знання у професійній діяльності. Індивідуальна робота студента є засобом оволодіння навчальним матеріалом самостійно у вільний від обов'язкових навчальних занять час.

Загальна **процедура виконання студентом індивідуального завдання** охоплює декілька етапів:

1. Попереднє ознайомлення із змістом завдання. На цьому етапі студент повинен усвідомити місце завдання у навчальній програмі дисципліни.

2. На другому етапі відбувається детальний аналіз змісту завдання. Основою цього етапу роботи є знання, які вже має студент. Студент демонструє своє бачення проблематики ситуації, способів її розв'язання.

3. Третій етап полягає у розв'язанні поставленого перед студентом завдання.

4. На четвертому етапі студент повинен перевірити правильність ходу міркувань та проаналізувати отримані результати.

5. Підготовка звіту.

Структура індивідуального навчально-дослідного завдання (орієнтовна):

- титульна сторінка (додаток А);
- вступ, де зазначається мета та завдання роботи.

- теоретичне обґрунтування – виклад базових теоретичних положень, алгоритмів тощо, на основі яких виконується завдання;
- основні результати роботи;
- висновки;
- список використаної літератури.

Форми контролю індивідуальної навчально-дослідної роботи: розв'язане практичне завдання, звіт.

2. ЗМІСТ ІНДИВІДУАЛЬНИХ НАВЧАЛЬНО-ДОСЛІДНИХ ЗАВДАНЬ І МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ЇХ ВИКОНАННЯ

Теми рефератів

1. Побудова ефективних рубежів територіального захисту і доступ до незахищених інформаційних ресурсів.
2. Протидія розкраданню документів та електронних носів інформації.
3. Методи протидії візуальному перехопленню інформації з екранів моніторів.
4. Боротьба з прослуховуванням (методика, будова і оптимізація захисних бар'єрів).
5. Системи оптичного і акустичного екранування носіїв інформації з обмеженим доступом.
6. Атестація систем захисту інформації на підприємстві.
7. Порядок і методи контролю за станом фізичного захисту інформаційно-комунікаційних систем.
8. Захист інформації в системах перетворення, опрацювання, пересилання і приймання відеоканалів, що містять конфіденційну інформацію.
9. Біометричні системи доступу до захищених інформаційних систем.
10. Мінімальні стандарти організаційних основ захисту інформації з обмеженим доступом в країнах НАТО і ЄС.
11. Стандарт ISO/IES (27001: «Інформаційні технології – Методика безпеки – Система менеджменту – Вимоги» (стандарт, за яким організація може бути сертифікована).
12. Стандарт ISO/IES (27005:2008 «Інформаційні технології – Методика безпеки – Управління ризиками інформаційної безпеки» (стандарт, що надає рекомендації з управління безпекою на основі підходу управління ризиками).
13. Стандарт ISO/IES (27006:2007 «Інформаційні технології – Методика безпеки – Вимоги до організацій, що проводять аудит і організацію систем менеджменту інформаційної безпеки» (настанови з акредитації сертифікаційних організацій).
14. Вимоги до обладнання, приладів і метрологічного забезпечення робіт в комплексній інформаційно-комунікаційній системі захисту інформації.
15. Американська модель управління персоналом підприємства.
16. Японська модель управління персоналом підприємства.

17.Загальні критерії, що висуваються до співробітників служби безпеки типової фірми США.

18. Критерії та основні підбору працівників для виробництва у США.

19. Тренінг з питань захисту комерційної таємниці та забезпечення безпеки фірми в США.

20. Проблемно-орієнтовані семінари в галузі захисту комерційної таємниці фірм (на прикладі США).

21.Криптографічний захист на основі еліптичних кривих.

Список рекомендованої літератури

1. Бармен С. Разработка правил информационной безопасности / С. Бармен. – К.: “Вильямс”, 2002. – 208 с.
2. Батюк А. С. та ін. Інформаційні системи в менеджменті: навч. посіб. / А. С. Батюк, З. П. Двуліт, К. М. Обельовська, І. М. Огородник, Л. П. Фабрі. – Львів: Національний університет “Львівська політехніка (Інформаційно-видавничий центр “Інтелект+” Інституту післядипломної освіти), “Інтелект-Захід”, 2004. – 520 с.
3. Галатенко В. А. Основы информационной безопасности: курс лекций: учеб. пособ. / под ред. В. Б. Бетелина. Изд. 3-е. М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. 208 с.
4. Годин В. В., Корнеев И. К. Информационное обеспечение управленческой деятельности: учеб. / В. В. Годин, И. К. Корнеев. – М.: Мастерство; Высшая школа, 2001. – 240 с.
5. Гужва В. М. Інформаційні системи і технології на підприємствах: навч. посіб. / В. М. Гужва. – К.: КНЕУ, 2001. – 400 с.
6. Гундарь К. Ю. та ін. Защита информации в компьютерних системах / К. Ю. Гундарь, А. Ю. Гундарь, Д. А. Янишевский. – К.: “Корнійчук”, 2000. – 152 с.
7. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Чинний з 29.12.2014 р. ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. 228 с.
8. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція хешування. – Чинний з 29.12.2014 р. – ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. – 228 с.
9. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. К. : Держстандарт України, 2003.
10. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу. – Чинний з 28.04.1999. – К.: ДСТСЗІ СБ України, 1999. – 14 с.
11. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. – Чинний з 28.04.1999. – К.: ДСТСЗІ СБ України, 1999. – 53 с.

12.Зелинский С. Э. Internet для каждого / С.Э. Зелинский. – К.: Юниор, 2001. – 368 с.
13.Інформаційна безпека: навч. посіб. / С. В. Кавун, В. В. Носов, О. В. Манжай. Харків: Вид. ХНЕУ, 2008. – 352 с.
14.Інформаційні системи і технології в економіці / за ред. В. С. Пономаренка. – К.: ВЦ "Академія", 2002. – 544 с.
15.Кавун С. В. Информационная безопасность в бизнесе: науч. изд. Харьков: Изд. ХНЕУ, 2007. – 408 с.
16.Кузнецов О. О. Захист інформації в інформаційних системах: навч. посіб. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Харків: ХНЕУ, 2011. – 510 с.
17.Ляшенко І.О. Європейські критерії безпеки інформаційних технологій / І.О. Ляшенко // Сучасні інформаційні технології у сфері безпеки та оборони. – 2012. – № 1 (13). – С. 84–86.
18.Остапов С.Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с. URL: https://www.twirpx.com/file/2340575/
19.Попов В. Практикум по Internet-технологиям / В. Попов. – Санкт-Петербург.: Питер, 2002. – 480 с.
20.Про захист інформації в інформаційно-комунікаційних системах: Закон України від № 80/94ВР. Відомості Верховної Ради України. 1994. № 31. ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр
21. Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. Відомості Верховної Ради України. 2017, № 45, ст. 400. URL: https://zakon.rada.gov.ua/laws/show/2155-19.
22.Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
23.Токен – новий вид інформації. Газета «Інтерактивна бухгалтерія» №128 /2019. URL: https://interbuh.com.ua/ua/documents/oneanalytics/131413
24.Хорошко В.О. Основи інформаційної безпеки: підручник / В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест; за ред. В.О. Хорошка. – К.: ДУІКТ, 2008. – 186 с.
25.Юринець В. С., Гончарук Я. Л. Основи автоматизованих інформацій-них систем: навч. посіб. / В. С. Юринець, Я. Л. Гончарук. – Л.: ЛНУ, 2001. – 256 с.

3. ПОРЯДОК ОФОРМЛЕННЯ ТА ЗАХИСТУ ІНДИВІДУАЛЬНИХ НАВЧАЛЬНО-ДОСЛІДНИХ ЗАВДАНЬ

1. Звіт про виконання ІНДЗ подається у друкованому форматі на папері формату А4.

Оформлення звіту: шрифт − Times New Roman; розмір шрифту − 14 кегель; інтервал між рядками − півтора; абзац − 12,5 мм, поля: верхнє і нижнє – 20 мм, ліве – 25 мм, праве – 15 мм; нумерація сторінок − по центру нижнього поля. Зразок оформлення титульної сторінки наведено у додатку А.

2. ІНДЗ подається викладачу не пізніше ніж за 1 тиждень до заліку в друкованому вигляді (звіт).

3. Оцінка за ІНДЗ виставляється на заключному занятті з навчальної дисципліни на основі попереднього ознайомлення викладача зі змістом ІНДЗ.

4. Оцінка за ІНДЗ є обов'язковою складовою підсумкової оцінки з навчальної дисципліни.

4. КРИТЕРІЇ ОЦІНЮВАННЯ

Результати індивідуальної роботи оцінюються викладачем згідно з чинною шкалою оцінювання.

№ з/п	Види робіт. Критерії оцінювання знань студентів	Бали рейтингу	Максимальна кількість балів
Індивідуальна робота студента (ІНДЗ)			
Критерії оцінювання		**5 балів**	
завдання виконане у зазначений термін, у повному обсязі і без помилок		**5**	
завдання виконане у зазначений термін, у повному обсязі, але є незначні помилки		**4**	
завдання виконане у неповному обсязі, або (та) з порушенням терміну виконання, або (та) при наявності значних помилок		**3**	
завдання виконане із суттєвими помилками		**2**	
завдання не виконане або тільки розпочато його розв'язання		**0-1**	

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Кафедра цифрової економіки та бізнес-аналітики

Індивідуальне навчально-дослідне завдання

з дисципліни

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Виконав:

Перевірив:

Львів – 202_