МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

ФАКУЛЬТЕТ УПРАВЛІННЯ ФІНАНСАМИ ТА БІЗНЕСУ

КАФЕДРА ЦИФРОВОЇ ЕКОНОМІКИ ТА БІЗНЕС-АНАЛІТИКИ

ЗАТВЕРДЖЕНО

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

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

КОМПЛЕКТ КОНТРОЛЬНОЇ РОБОТИ 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

ВАРІАНТ №1

І рівень завдання з вибором відповіді – тестові завдання. Завдання з вибором відповіді вважається виконаним правильно, якщо студентом вказана вірна відповідь. За кожне правильно виконане завдання виставляється 0,2 бали	
1.	**Які існують способи компроментації електронного цифрового підпису?** а) традиційні; б) відкриті; в) доступні; г) фальсифіковані.
2.	**Виберіть правильну відповідь, якою слід продовжити наступне твердження «Несанкціонований доступ може здійснюватись за допомогою…»** а) програмно-апаратного забезпечення, яке включене до складу комп'ютерної системи; б) ряду організаційних, технічних та правових заходів; в) реалізації функції проникнення та знищення чи модифікації файлів; г) правильна відповідь відсутня.
3.	**Назвіть узагальнену категорію методів захисту від несанкціонованого доступу:** а) організаційна; б) законодавча; в) асоціативна; г) надійна.
4.	**Вкажіть, що з наведеного переліку відноситься до методів реалізації несанкціонованого доступу до інформації:** а) троянський кінь, атака, розрив лінії; б) троянський кінь, логічна бомба, екранування; в) логічна бомба, екранування, маскарад; г) екранування, маскарад, маскування.
5.	**Якщо для кожного повідомлення в процесі шифрування використовується новий ключ – він називається:** а) динамічний; б) статичний; в) ключовий; г) публічний.
6.	**Назвіть, який існує метод шифрування інформації:** а) динамічний; б) автоматизований; в) симетричний; г) опублікований.
7.	**Назвіть переваги використання несиметричного методу шифрування:** а) використання закритого ключа дозволяє ідентифікувати відправника зашифрованого повідомлення; б) використання відкритого ключа дозволяє ідентифікувати зашифроване повідомлення; в) взаємний обмін відкритими ключами між партнерами дозволяє їм створити захищений спрямований канал зв'язку між ними; г) подвійне послідовне шифрування дозволяє партнерам створити спрямований канал зв'язку.
8.	**Що з переліченого не відноситься до традиційних способів компроментації ЕЦП?** а) викрадення закритого ключа шляхом незаконного копіювання; б) викрадення закритого ключа разом з устаткуванням; в) реконструкція закритого ключа; г) заволодіння ключем в результаті змови з особами, які мають право на його

	використання.
9.	**Назвіть узагальнену категорію методів захисту від несанкціонованого доступу:** а) технологічна; б) законодавча; в) асоціативна; г) умовно надійна.
10.	**Назвати, які ключі використовуються для шифруванні інформації несиметричний методом:** а) відкритий; б) динамічний; в) статичний; г) особистий; д) незалежний.
Другий рівень – завдання з короткою відповіддю. Завдання з короткою відповіддю вважається виконаним правильно, якщо студент дав вірні визначення, посилання, тлумачення, короткі коментарі. За кожне правильно виконане завдання виставляється 0,5 бали	
1.	Для чого використовується е-токен? Які його види існують?
2.	Опишіть асиметричний метод шифрування.
Третій рівень – завдання із розгорнутою відповіддю За правильно виконане завдання виставляється 2 бали.	
1.	Використовуючи ключ довжиною 3, продемонструвати приклад роботи методу Віженера.
РАЗОМ:	**5 балів**

Укладач:_____ Задорожна А. В., доцент кафедри цифрової економіки та бізнес-аналітики
(підпис) (ПІБ, посада, науковий ступінь, вчене звання)

КРИТЕРІЇ ОЦІНЮВАННЯ

№ з/п	Види робіт. Критерії оцінювання знань студентів	Бали рейтингу	Максимальна кількість балів
Критерії оцінювання		**5 балів**	
Встановлено 3 рівні складності завдань. **1. Перший рівень (завдання 1) – завдання із вибором відповіді – тестові завдання.** Завдання з вибором відповіді на теоретичне питання вважається виконаним правильно, якщо в картці тестування записана правильна відповідь.		0,2 (за одне завд.) × 10 завдань = 2	
2. Другий рівень (завдання 2) – завдання з короткою відповіддю. Завдання з короткою відповіддю вважається виконаним правильно, якщо студент дав вірні визначення, посилання, тлумачення, короткі коментарі.		0,5 (за одне завд.) × 2 завдання = 1	
3. Третій рівень (завдання 3) – тестові завдання практичної направ-леності. Завдання з вибором відповіді на практичне питання вважається виконаним правильно, якщо в картці тестування записана правильна відповідь.		2 (за одне завд.) × 1 завдання = 2	

ПЕРЕЛІК ДОВІДКОВОЇ ЛІТЕРАТУРИ

1. Алферов А.П. Основы криптографии: учеб. пособ. / А.П.Алферов, А.Ю.Зубов, А.С.Кузьмин, А.В.Черемушкин. – М.: Гелиос АРВ, 2002 – 480 с.
2. Басалова Г.В. Основы криптографии / Г.В. Басалова. – М.: Национальный Открытый Университет "ИНТУИТ", 2016. – 283 с. URL: https://www.twirpx.com/file/1907188/
3. Воробьев С.П., Орловский Н.М. Зашита информации: учеб. пособ. / С.П. Воробьев, Н.М. Орловский. ЮРГПУ (НПИ) им.М.И.Платова. – Новочеркасск: ЮРГПУ(НПИ), 2015.– 27 с.
4. Вострецова Е. В. Основы информационной безопасности : учеб. пособ. / Е.В. Вострецова. – Екатеринбург : Изд-во Урал.ун-та, 2019. – 204 с.
5. 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.
6. Дорошенко А. Н. Информационная безопасность. Методы и средства защиты информации в компьютерных системах : учебн. пособ. / А. Н. Дорошенко, Л. Л. Ткачев. – М. : МГУПИ, 2006. – 143 с.
7. Кавун С. В. Информационная безопасность в бизнесе: науч. изд. Харьков: Изд. ХНЕУ, 2007. – 408 с.
8. 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/
9. 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.