МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ М.П. ДРАГОМАНОВА

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ОСВІТНІХ ВИМІРЮВАНЬ

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

ПРОГРАМА

нормативної навчальної дисципліни

(дисципліни професійної та практичної підготовки)

підготовки **бакалавра**

галузь знань **12 Інформаційні технології**

спеціальність **121 Інженерія програмного забезпечення**

КИЇВ – 2019

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ М.П. ДРАГОМАНОВА

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ОСВІТНІХ ВИМІРЮВАНЬ

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

ПРОГРАМА

нормативної навчальної дисципліни

(дисципліни професійної та практичної підготовки)

підготовки **бакалавра**

галузь знань **12 Інформаційні технології**

спеціальність **121 Інженерія програмного забезпечення**

КИЇВ – 2019

УДК 004.056 (073)
Б39

Рекомендовано до друку Вченою радою Факультету інформатики Національного педагогічного університету імені М.П. Драгоманова (протокол № 3 від 19 грудня 2018 р.).

Рекомендовано до друку Вченою радою Національного педагогічного університету імені М.П. Драгоманова (протокол № 10 від 28 березня 2019 р.).

Рецензенти:

Ю.В. Триус — доктор педагогічних наук, професор, завідувач кафедри комп'ютерних наук та системного аналізу Черкаського державного технологічного університету.

В.Я. Кархут — кандидат педагогічних наук, доцент кафедри програмної інженерії Факультету інформатики НПУ імені М.П. Драгоманова.

Б39 Безпека програм та даних: програма навчальної дисципліни для підготовки студентів за спеціальністю «121 Інженерія програмного забезпечення» Факультету інформатики НПУ імені М.П. Драгоманова / укл. В.М. Франчук (в авторській редакції). - Київ: Вид-во НПУ імені М.П. Драгоманова, 2019 р. – 30 с.

В програмі наведено зміст навчальної дисципліни «Безпека програм та даних» для підготовки студентів за спеціальністю «121 Інженерія програмного забезпечення» Факультету інформатики НПУ імені М.П. Драгоманова. Програма складена за модульною схемою, наведено завдання вивчення навчальної дисципліни, вимоги до знань, навичок та умінь студентів, інформаційне наповнення, тематика лабораторних занять, зразки підсумкового контролю навчальних досягнень студентів, список рекомендованої літератури. Може бути використана для підготовки студентів фізико-математичних та інформатичних спеціальностей педагогічних закладів вищої освіти.

УДК 004.056 (073)

ЗМІСТ

ВСТУП

Програма навчання нормативної дисципліни «*Безпека програм та даних*» складена відповідно до освітньо-професійної програми підготовки бакалавра з галузі знань «12 Інформаційні технології» спеціальності «121 Інженерія програмного забезпечення» і є основним документом, в якому визначається обсяг і орієнтовний порядок вивчення змістових модулів навчальної дисципліни відповідно до галузевого стандарту вищої освіти.

Навчання дисципліни «*Безпека програм та даних*» дає студентам необхідні теоретичні знання про основні принципи апаратно-програмних засобів захисту даних в комп'ютерних системах, криптографічних та стеганографічних методів захисту даних, що сприяє формуванню інформатичних компетентностей майбутніх фахівців.

Предметом навчання дисципліни є процес формування у майбутніх фахівців з розробки та тестування програмного забезпечення знань, умінь та навичок захисту програм та даних.

Міждисциплінарні зв'язки. Одним із важливих компонентів програми є міжпредметне узгодження. Курс «*Безпека програм та даних*» розрахований для студентів, що засвоїли базові математичні курси та вивчили дисципліни «Конструювання програмного забезпечення», «Архітектура комп'ютера», «Операційні системи», «Організація комп'ютерних мереж» і мають базові знання про склад і призначення основних компонентів обчислювальної техніки. Вивчення даного курсу забезпечує необхідний рівень знань для опанування дисциплінами «Якість програмного забезпечення та тестування», «Архітектура та проектування програмного забезпечення», «Програмування Інтернет».

Програма навчальної дисципліни «*Безпека програм та даних*» складається з таких змістових модулів:

I. Апаратно-програмні засоби захисту даних в комп'ютерних системах.
II. Криптографічні та стеганографічні методи захисту даних.

1. Мета та завдання навчальної дисципліни

Метою навчання дисципліни «*Безпека програм та даних*» є формування у студентів за напрямом підготовки бакалавра з галузі знань «12 Інформаційні технології» спеціальності «121 Інженерія програмного забезпечення» системи фундаментальних знань щодо свідомого, активного та вмілого використання нових інформаційних технологій захисту даних у процесі розробки та тестування програмного забезпечення..

Основними завданнями навчання дисципліни «*Безпека програм та даних*» є:

- розкрити місце і значення дисципліни в загальній і професійній діяльності;
- з'ясувати психолого-педагогічні аспекти засвоєння предмету, взаємозв'язки курсу з іншими навчальними дисциплінами, зокрема з інформатичними дисциплінами;
- навчити студентів ефективно захищати дані під час розробки та тестування програмного забезпечення;
- навчити майбутніх фахівців орієнтуватися у засобах захисту комп'ютерних систем, свідомо обирати тип, склад та конфігурацію обчислювальної техніки у відповідності до конкретних вимог використання цих систем;
- продемонструвати ефективність використання методів захисту програм та даних.
- розглянути криптографічні та стеганографічні методи захисту програм та даних.

Основні результати навчання і компетентності згідно з вимогами освітньо-професійної програми. Дисципліна є методичною і практичною основою сукупності знань та вмінь, необхідних майбутньому фахівцеві для виконання професійних завдань, пов'язаних з використанням апаратно-програмних засобів захисту даних в комп'ютерних системах у своїй професійній діяльності.

№ з/п	Результати навчання	Компетентності
1	**Знати:** − актуальні проблеми комп'ютерної безпеки, цілісність даних,	**Соціально-особистісні:** − здатність учитися; − турбота про якість

	конфіденційність даних, доступність даних, розголошення даних, витік даних, захист даних, порушенням режиму доступу, несанкціонований доступ, об'єкт злочину, блокування даних, модифікація даних, одержання захищуваних даних, фільтрація даних, канал витоку даних, помилка, прорахунок, вразливість інформаційної системи, види загроз, джерела загроз, контроль безпеки, види атак, вторгнення, політика безпеки, класифікація навмисних загроз безпеки комп'ютерних систем; − стискування, архівація даних, архіватор, ступінь стискування, коефіцієнт стискування, методи стискування файлів, резервне копіювання, технології резервного копіювання; − перспективні розробки у сфері зберігання вмісту запам'ятовуючих пристроїв, технології захисту оптичних дисків від несанкціонованого копіювання, діагностика та профілактика жорстких магнітних дисків, технології захисту флеш-накопичувачів, засоби відновлення пошкодженого і втраченого вмісту запам'ятовуючих пристроїв, гарантоване вилучення вмісту запам'ятовуючих пристроїв; − вразливості програмного забезпечення та засоби боротьби з ними, дослідження вихідних текстів програмного забезпечення, захист	виконуваної роботи. **Загальнонаукові:** − базові знання в галузі захисту інформаційних ресурсів; − навички використання програмних засобів і навички роботи в комп'ютерних системах, уміння використовувати засоби захисту даних. **Інструментальні:** − навички роботи захисту даних під час роботи за комп'ютером; − навички роботи захисту даних під час роботи з інформаційними ресурсами; − дослідницькі навички у галузі захисту даних. **Професійні:** − розуміння тенденцій розвитку захисту інформаційних ресурсів; − вміння застосовувати захист інформаційних ресурсів в наукових дослідженнях та в професійній діяльності; − здатність до ділових комунікацій у

	програм встановлених на жорсткому диску, захист програм від вивчення; − комп'ютерні віруси і засоби боротьби з ними, історія комп'ютерних вірусів, класифікація комп'ютерних вірусів, антивірусні програми, типи антивірусних програм, методи розпізнавання шкідливих об'єктів, захист комп'ютера від шпигунських програм; − мережеві атаки, види мережевих атак, сегментація мереж, міжмережеві екрани, списки управління доступом (ACL), загрози використання глобальної мережі Інтернет, методи захисту; − актуальні проблеми використання безпровідних мереж, типи загроз безпеці в безпровідних мережах, способи захисту даних в безпровідних мережах. **Вміти:** − використовувати засоби парольної ідентифікації в операційних системах, в програмних додатках, в мережевих сервісах, способи захисту від перебирання паролів, варіанти заміни традиційних паролів, способи створення складних паролів; − застосовувати засоби захисту і спеціалізовані програмні продукти для розв'язування типових проблем в галузі захисту інформаційних ресурсів; − кваліфіковано оцінювати можливості застосування конкретних	професійній сфері, знання основ ділового спілкування, здатність до роботи в команді для захисту інформаційних ресурсів.

	механізмів захисту; − компетентно використовувати апаратні та програмні засоби захисту при розв'язуванні практичних задач.	
2	**Знати** − поняття криптології, криптографії. Ключ, шифрування, зашифровування, розшифровування, криптостійкість, криптоаналіз, методи криптоаналізу, криптографічні методи захисту даних; − алгоритми шифрування, симетричні криптографічні алгоритми, асиметричні криптографічні алгоритми; − криптосистеми з відкритим ключем, електронний (цифровий) підпис, технології застосування систем електронного цифрового підпису, генерація ключів; − реалізації криптозахисту на апаратному рівні. Архітектура апаратних засобів криптозахисту. Організація інтерфейсу для роботи з прикладними програмами; − поняття стеганографії, історія стеганографії, стеганографічні методи і системи; − проблеми шифрування великих повідомлень, сучасні способи вирішення проблеми розподілу ключів, системи біометричної аутентифікації, перспективи використання криптографічних засобів захисту даних. **Вміти** − застосовувати симетричні криптографічні алгоритми,	**Соціально-особистісні:** − здатність учитися; − турбота про якість виконуваної роботи. **Загальнонаукові:** − базові знання в галузі захисту інформаційних ресурсів; − навички використання програмних засобів і навички роботи в комп'ютерних системах, уміння використовувати засоби захисту даних. **Інструментальні:** − навички роботи захисту даних під час роботи за комп'ютером; − навички роботи захисту даних під час роботи з інформаційними ресурсами; − дослідницькі навички у галузі захисту даних. **Професійні:** − розуміння тенденцій розвитку захисту інформаційних ресурсів;

	асиметричні криптографічні алгоритми; − користуватися криптосистеми з відкритим ключем, електронний (цифровий) підпис, технології застосування систем електронного цифрового підпису, генерація ключів; − використовувати стеганографічні методи і системи.	− вміння застосовувати захист інформаційних ресурсів в наукових дослідженнях та в професійній діяльності; − здатність до ділових комунікацій у професійній сфері, знання основ ділового спілкування, здатність до роботи в команді для захисту інформаційних ресурсів.

Дисципліна «*Безпека програм та даних*» за навчальним планом підготовки бакалавра належить до нормативної складової циклу професійної та практичної підготовки. На вивчення курсу «*Безпека програм та даних*», який вивчається на 3 та 4 курсі (7, 8 семестр), відводиться 4 кредити або 120 навчальні години, з яких 76 годин відведено на самостійну навчально-пізнавальну роботу студентів, а 44 години – на аудиторні заняття, які проводяться у формі лекційних занять (16 год.) та лабораторних робіт (28 год.). Самостійна робота полягає у підготовці до аудиторних занять, виконанні завдань, що пропонуються на лекційних та лабораторних заняттях, підготовці до модульного контролю тощо.

Шифр	***Назва дисципліни***	***Вид контролю***	***ECTS***	***Всього***	***Самостійна робота***	***Аудиторні***	***Лекції***	***Лабораторні***	***Індивідуальні***
ПП05	Безпека програм та даних	Екзамен (7,8 сем.)	4	120	76	44	16	28	0

На лекційних заняттях розглядаються фундаментальні теоретичні питання з безпеки програм та даних; систематизуються, та

узагальнюються знання, навички та уміння набуті при вивченні суміжних дисциплін.

На лабораторних заняттях студенти знайомляться із сучасними програмними і апаратними засобами захисту даних, набувають уміння і навички роботи із ними. Одним із основних завдань при проведенні лабораторного практикуму є набуття умінь та навичок аналізу роботи програмного засобу та апаратного забезпечення під його управлінням, умінь виконувати його налагодження і адаптацію до вирішення задач у наступній професійній діяльності чи повсякденному житті. Метою проведення лабораторних занять є розвиток у студентів навичок самостійного використання набутих знань, навичок та умінь і забезпечення засвоєння основних понять навчальної дисципліни.

Викладання навчального курсу супроводжується з використанням навчально-методичної літератури, перелік якої додається, виконанні розроблених завдань до лабораторних робіт, технічними засобами навчання, спеціальним програмним забезпеченням. В системі управління навчальними ресурсами MOODLE розміщено теоретичні відомості та завдання до лабораторних занять.

На консультаціях зі студентами передбачається з'ясування і обговорення проблемних питань, що стосуються виконання самостійних завдань до лекційних і лабораторних занять, незрозумілих студентами теоретичних питань тощо. Реалізація вищезгаданих вимог забезпечує один з головних напрямків професійної підготовки сучасного фахівця і дозволяє йому активно використовувати сучасні технології захисту даних під час розробки та тестування програмного забезпечення.

2. Інформаційний обсяг навчальної дисципліни

Зміст курсу «*Безпека програм та даних*» подано у вигляді модулів, до кожного з яких наведено перелік основних термінів та понять, що студенти повинні знати та основних вмінь, якими вони повинні оволодіти після вивчення відповідного модуля, а також тематику занять та анотації до них.

2.1. Структура навчальної дисципліни

Змістовий модуль 1. Апаратно-програмні засоби захисту даних в комп'ютерних системах.

Тема 1. *Основні поняття з галузі захисту інформаційних ресурсів.*

Зміст теми: Актуальність проблеми комп'ютерної безпеки, цілісність даних, конфіденційність даних, доступність даних, розголошення даних, витік даних, захист даних, порушенням режиму доступу, несанкціонований доступ, об'єкт злочину, блокування даних, модифікація даних, одержання захищуваних даних, фільтрація даних, канал витоку даних, помилка, прорахунок, вразливість інформаційної системи, види загроз, джерела загроз, контроль безпеки, види атак, вторгнення, політика безпеки, класифікація навмисних загроз безпеки комп'ютерних систем.

Тема 2. *Засоби парольної ідентифікації та адміністрування.*

Зміст теми: Ідентифікація, засоби парольної ідентифікації в операційних системах, в програмних додатках, в мережевих сервісах, способи захисту від перебирання паролів, варіанти заміни традиційних паролів, способи створення складних паролів.

Тема 3. *Архівування та резервне копіювання даних.*

Зміст теми: Стискування, архівація даних, архіватор, ступінь стискування, коефіцієнт стискування, методи стискування файлів, резервне копіювання, технології резервного копіювання.

Тема 4. *Захист вмісту зовнішньої пам'яті.*

Зміст теми: Перспективні розробки у сфері зберігання вмісту запам'ятовуючих пристроїв, технології захисту оптичних дисків від несанкціонованого копіювання, діагностика та профілактика жорстких магнітних дисків, технології захисту флеш-накопичувачів, засоби відновлення пошкодженого і втраченого вмісту запам'ятовуючих пристроїв, гарантоване вилучення вмісту запам'ятовуючих пристроїв.

Тема 5. *Захист програмного забезпечення.*

Зміст теми: Вразливості програмного забезпечення та засоби боротьби з ними, дослідження вихідних текстів програмного забезпечення, захист програм встановлених на жорсткому диску, захист програм від вивчення.

Тема 6. *Захист вмісту запам'ятовуючих пристроїв від шкідливих програм.*

Зміст теми: Комп'ютерні віруси і засоби боротьби з ними, історія комп'ютерних вірусів, класифікація комп’ютерних вірусів, антивірусні програми, типи антивірусних програм, методи

розпізнавання шкідливих об'єктів, захист комп'ютера від шпигунських програм.

Тема 7. *Поширені види мережевих атак і способи захисту від них.*

Зміст теми: Мережеві атаки, види мережевих атак, сегментація мереж, міжмережеві екрани, списки управління доступом (ACL), загрози використання глобальної мережі Інтернет, методи захисту.

Тема 8. *Організація бездротового зв'язку, специфічні атаки на бездротові мережі та способи захисту від них.*

Зміст теми: Актуальні проблеми використання безпровідних мереж, типи загроз безпеці в безпровідних мережах, способи захисту даних в безпровідних мережах.

Змістовий модуль 2. Криптографічні та стеганографічні методи захисту даних.

Тема 9. *Основні поняття криптографії. Коротка історія криптографії.*

Зміст теми: Поняття криптології, криптографії. Ключ, шифрування, зашифровування, розшифровування, криптостійкість, криптоаналіз, методи криптоаналізу, криптографічні методи захисту даних.

Тема 10. *Популярні алгоритми шифрування даних.*

Зміст теми: Алгоритми шифрування, асиметричні криптографічні алгоритми, симетричні криптографічні алгоритми.

Тема 11. *Використання електронного підпису.*

Зміст теми: Криптосистеми з відкритим ключем, електронний (цифровий) підпис, технології застосування систем електронного цифрового підпису, генерація ключів.

Тема 12. *Програмно-апаратні засоби шифрування даних.*

Зміст теми: Реалізації криптозахисту на апаратному рівні. Архітектура апаратних засобів криптозахисту. Організація інтерфейсу для роботи з прикладними програмами.

Тема 13. *Основні поняття стеганографії. Історія стеганографії. Стеганографічні методи і системи.*

Зміст теми: Поняття стеганографії, історія стеганографії, стеганографічні методи і системи.

Тема 14. *Деякі проблеми і перспективи використання*

криптографічних засобів захисту даних.

Зміст теми: Проблеми шифрування великих повідомлень, сучасні способи вирішення проблеми розподілу ключів, системи біометричної аутентифікації, перспективи використання криптографічних засобів захисту даних.

2.2. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Засоби парольної ідентифікації та адміністрування.	2
2	Архівування та резервне копіювання даних.	2
3	Захист вмісту зовнішньої пам'яті.	2
4	Захист програмного забезпечення.	2
5	Захист даних від шкідливих програм.	2
6	Поширені види мережевих атак і способи захисту від них.	2
7	Організація бездротового зв'язку, специфічні атаки на бездротові мережі та способи захисту від них.	2
8	Потокові криптографічні алгоритми. (Шифри Цезаря, Трітеміуса, Полібія).	2
9	Потокові криптографічні алгоритми. (Плейфера, «подвійний квадрат» Уітстона, Вернама).	2
10	Блокові криптографічні алгоритми. (Шифри скітала («палиця»), стандартної та вертикальної перестановки комбінованих перестановок).	2
11	Блокові криптографічні алгоритми. (Шифри-трафарети. Квадрат та прямокутник Кардано).	2
12	Змішані симетричні криптосистеми. (Багатоалфавітна криптосистема Віженера).	2
13	Асиметричні і гібридні криптосистеми.	2
14	Криптографічні та стеганографічні програмні засоби.	2

2.3. Самостійна (індивідуальна) робота

Перелік тем, винесених на самостійне опрацювання

№ Самостійної роботи	Теми	Бали
1	• Концепція інформаційної безпеки: стратегія і тактика.	8

	• Інформаційна безпека: поняття, сутність та значення. • Аудит інформаційної безпеки. • Інформаційна безпека в аспекті соціальної діяльності. • Організаційно-управлінські заходи забезпечення інформаційної безпеки.	
2	• Електронний бізнес та інформаційна безпека. • Співвідношення категорій «інформаційна безпека» та «захист даних». • Інформатизація її вплив на інформаційну безпеку. • Принципи організації інформаційної безпеки та захисту даних. • Визначення критеріїв та аналіз оперативного стану інформаційної безпеки.	8
3	• Захист даних в соціальних мережевих сервісах. • Класифікація злочинів у сфері інформаційних правовідносин. • Комп'ютерні злочини та захист даних. • Комп'ютерна злочинність та комп'ютерна безпека. • Виявлення та розслідування комп'ютерних злочинів.	8
4	• Протидія комп'ютерним злочинам. • Інженерно-технічний захист даних: сутність та загальна характеристика. • Фізичні засоби захисту даних. • Апаратні засоби захисту даних. • Програмні засоби захисту даних. • Технічні канали витоку даних. • Інженерно-технічні заходи забезпечення інформаційної безпеки. • Програмно-апаратний захист даних. • Програмно-апаратні засоби шифрування даних. • Організаційно-технічні (інженерно-технологічні) заходи забезпечення інформаційної безпеки. • Поняття та сутність організації технічного захисту	

	даних в автоматизованих системах. • Організація інформаційної безпеки інженерно-технічними засобами. • Способи несанкціонованого доступу технічними засобами до інформаційних систем та їх класифікація.	
	Всього	***32***

Методичні рекомендації до написання реферату

Реферат (лат. referre - доповідати, повідомляти) підводить підсумок вивчення студентами як окремої теми (самостійна робота), так і дисципліни в цілому.

Обсяг реферату визначається специфікою досліджуваного питання і змістом матеріалів (документів), їх науковою цінністю та практичним значенням. Оптимальний обсяг реферату складає 10-15 сторінок. **Реферат має відповідати вимогам до оформлення рукопису кваліфікаційної роботи:** *вступ і висновки в сумі не повинні перевищувати 20% від її загального обсягу; текст друкується через 1,5 інтервали на одній сторінці стандартного аркуша з такими полями: ліве - 30 мм, праве - 15 мм, верхнє - 20 мм, нижнє - 20 мм; всі сторінки нумеруються: загальна нумерація починається з титульного листа, проте порядковий номер на ньому не ставиться.*

На титульному листі реферату вказуються: *офіційна назва закладу освіти, інституту (факультету) і кафедри; прізвище та ініціали автора реферату (абревіатура навчальної групи); повна назва теми; прізвище та ініціали наукового керівника, його науковий ступінь і вчене звання; місто, де знаходиться навчальний заклад та рік написання реферату*.

Після титульного листа подається зміст реферату з точною назвою кожного розділу (параграфу) і вказуванням його сторінок.

Список використаних джерел складається з дотриманням загальновизнаних вимог до робіт, що готуються до друку. До списку використаних джерел мають бути включені лише безпосередньо використані в рефераті праці в алфавітному порядку авторів. Монографії і збірники, що не мають на титульному аркуші прізвища автора (авторів), включаються до загального списку за алфавітним розміщенням заголовку.

Тема реферату – це не просто повторення засвоєного матеріалу лекції або семінарського заняття. Вона повинна являти собою самостійне розроблення проблеми, достатньо чітко окресленої від інших. Неприпустиме поєднання декількох проблем або, навпаки, штучне виокремлення певної частини єдиного питання.

Важливими критеріями при доборі теми реферату, є її актуальність, широка джерельна база, наявність необхідного фактичного матеріалу, а також достатнє її висвітлення в науково-методичній літературі, що передбачає, в першу чергу, ознайомлення із загальною концепцією автора праці та його висновками.

Структура реферату:

- титульний аркуш;
- зміст (план);
- вступ;
- розділи (вони часто поділяються на параграфи);
- висновки;
- список використаних джерел;
- додатки (у яких наводяться таблиці, схеми, діаграми тощо);
- перелік умовних позначень.

У вступі реферату обґрунтовується актуальність теми, її особливості, значущість з огляду на розвиток науки та практики або науково-методичної діяльності у сфері освіти. У вступі необхідно подати аналіз використаних джерел, назвавши при цьому авторів, які вивчали дану тематику, визначити сутність основних чинників, що вплинули та розвиток явища або процесу, що досліджується, на недостатньо досліджені питання, з’ясувавши причини їх слабкої аргументації.

Основну частину реферату складають кілька розділів (що можуть бути розбиті на параграфи), логічно поєднані між собою.

Виклад матеріалу в рефераті має бути логічним, послідовним, без повторень. Слід використовувати синтаксичні конструкції, характерні для стилю наукових документів, уникати складних граматичних зворотів, незвичних термінів і символів або пояснювати їх відразу, при першому згадуванні в тексті реферату. Терміни, окремі слова і словосполучення можна замінювати абревіатурами і сприйнятливими текстовими скороченнями, значення яких зрозуміле з контексту реферату.

Неприпустимо використовувати цитати без посилання на автора. При цитуванні будь-якого фрагменту джерела недопустимі неточності. Взагалі, цитатами не слід зловживати. Якщо якийсь важливий документ потребує наведення його в тексті реферату в повному обсязі, то краще винести його в додатки.

У рефераті необхідно визначити і викласти основні тенденції дослідження, підтвердити їх найтиповішими прикладами, відобразити сучасні ідеї та гіпотези, методики та методичні підходи до вивчення проблеми. Доцільно зупинитися на якомусь дискусійному моменті і спробувати проаналізувати позиції сторін, приєднавшись до однієї з них, чи висловити власну думку на певну проблему та визначити перспективи її вирішення.

Кожен розділ реферату повинен завершуватись короткими висновками, чіткими і лаконічними, де узагальнено оцінки та практичні рекомендації. Можна стисло вказати на перспективи подальшого дослідження даної проблеми.

Реферат оцінюється за такими критеріями: *актуальність; наукова та практична цінність; глибина розкриття теми, вирішення поставлених завдань; повнота використання рекомендованої літератури; обґрунтування висновків; грамотність; стиль викладу; оформлення реферату; обсяг виконаної роботи; завершеність дослідження*.

2.4. Методичне забезпечення

- Навчальна типова програма дисципліни.
- Робоча програма дисципліни.
- Плани занять.
- Навчальні-наочні посібники, технічні засоби навчання тощо.
- Конспект лекцій з дисципліни.
- Комплексні контрольні роботи (ККР) для визначення залишкових знань з дисципліни.
- Інструктивно-методичні матеріали лабораторних занять.
- Контрольні завдання до лабораторних занять.
- Методичні рекомендації та розробки викладача.
- Методичні матеріали, що забезпечують самостійну роботу студентів.

- Навчально-методична карта дисципліни:

Схема організації навчального процесу

Тиждень	Лекції	Бали	Лабораторні (практичні, семінарські) заняття, індивідуальні завдання, модульний контроль	Бали	Самостійна (індивідуальна) робота	Бали
Модуль 1. Апаратно-програмні засоби захисту даних в комп'ютерних системах (6 семестр)						
1	**Л.№1.** Вступ. Засоби парольної ідентифікації та адміністрування	5				
2	**Л.№2.** Архівування та резервне копіювання даних..	5				
3			**Л.Р.№1.** Засоби парольної ідентифікації та адміністрування.	10		
4	**Л.№3.** Захист вмісту зовнішньої пам'яті.	5				
5			**Л.Р.№2.** Архівування та резервне копіювання даних.	10	**С.Р.№1**	8
6	**Л.№4.** Захист програмного забезпечення. Захист даних від шкідливих програм.	5				
7			**Л.Р.№3.** Захист вмісту зовнішньої пам'яті.	10		
8	**Л.№5.** Поширені види мережевих атак і способи захисту від них. Специфічні атаки на бездротові мережі та способи захисту від них.	5				
9			**Л.Р.№4.** Захист програмного забезпечення.	10		
10			**Л.Р.№5** Захист даних від шкідливих програм.	10	**С.Р. №2**	8
11			**Л.Р.№6.** Поширені види мережевих атак і способи захисту від них.	10		
12			**Л.Р.№7.** Організація бездротового зв'язку, специфічні атаки на бездротові мережі та способи захисту від них.(По-бригадно).	10		
			Модульний контроль №1.	10		
Всього:		**25**	**Всього:**	**80**	**Всього:**	**16**

Всього за І модуль:						**121**
Модуль 2. Криптографічні та стеганографічні методи захисту даних (7 семестр)						
1	**Л.№6.** Основні поняття криптографії. Коротка історія криптографії.	5				
2	**Л.№7.** Популярні алгоритми шифрування даних (симетричні: потокові, блокові).	5				
3			**Л.Р.№8.** Потокові криптографічні алгоритми. (Шифри Цезаря, Трітеміуса, Полібія).	10	**С.Р. №3**	8
4	**Л.№8.** Популярні алгоритми шифрування даних (асиметричні). Використання електронного підпису.	5				
5			**Л.Р.№9.** Потокові криптографічні алгоритми. (Плейфера, «подвійний квадрат» Уітстона, Вернама).	10		
6	**Л.№9.** Основні поняття стеганографії. Історія стеганографії. Стеганографічні методи і системи.	5				
7			**Л.Р.№10.** Блокові криптографічні алгоритми. (Шифри скітала («палиця»), стандартної та вертикальної перестановки комбінованих перестановок).	10		
8	**Л.№10.** Стан та перспективи захисту даних.	5				
9			**Л.Р.№11.** Блокові криптографічні алгоритми. (Шифри-трафарети. Квадрат та прямокутник Кардано).	10	**С.Р. №4**	8
10			**Л.Р.№12.** Змішані симетричні криптосистеми. (Багатоалфавітна криптосистема Віженера).	10		
11			**Л.Р.№13.** Асиметричні і гібридні криптосистеми.	10		
12			**Л.Р.№14.** Криптографічні та стеганографічні програмні засоби.	10		
			Модульний контроль №2.	10		
Всього:		**25**	**Всього:**	**80**	**Всього:**	**16**

Всього за II модуль:					**121**
Всього за лекції	**50**	**Всього за лабораторні (практичні, семінарські) заняття**	**160**	**Всього за самостійну роботу**	**32**
Всього за семестр					**242**
Всього за лекції (100)	**21**	**Всього за лабораторні (практичні, семінарські) заняття (100)**	**66**	**Всього за самостійну роботу (100)**	**13**
Всього за семестр (100)					**100**
Екзамен					**100**
Оцінка за курс (середній бал)					**100**

Пояснення до схеми

1. Оцінювання лекційних занять:

№	Критерії	Бали
1	За відвідування.	2
2	За наявність конспекту лекції (Тести).	3
Всього:		**5**

Примітка: Перевірка записів конспекту здійснюється викладачем на останній лекції, в кінці кожного модуля або на останній лекції, в кінці семестру. Також може бути у формі тестових завдань.

2. Оцінювання лабораторних (практичних, семінарських) занять:

№	Критерії	Бали
1	За відвідування.	2
2	За теоретичні знання.	4
3	За виконання практичних завдань.	4
Всього:		**10**

Примітка: Захист лабораторних (практичних, семінарських) робіт здійснюється тільки на лабораторних (практичних, семінарських) заняттях згідно схеми організації навчального процесу.

3. Оцінювання самостійної (індивідуальної) роботи:

№	Критерії	Бали
1	За реферат.	4
2	За презентацію.	2
3	За виступ.	2
Всього:		**8**

Примітка: Потрібно опрацювати протягом семестру, як мінімум, 1 із тем, які винесені на самостійне опрацювання, і скласти її (їх) не пізніше завершення відповідного модуля згідно схеми організації навчального

процесу. Додаткові бали за самостійну роботу також можна отримати на лекційних та на лабораторних (практичних, семінарських) заняттях за активність при обговоренні навчального матеріалу.

Консультації проводяться на лекційних, лабораторних (практичних, семінарських) заняттях.

3. Рекомендована література

Основна:

1. Баричев СТ., Гончаров В.В., Серов Р.Е. Основы современной криптографии. М.: Горячая линия-Телеком, 2001. — 152 с.
2. Блэк У. Інтернет: протоколы безопасности. Учебный курс. — СПб.: Питер, 2010 — 288 с.
3. Болотов А.А., Гашков А.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. — М.: КомКнига, 2006. — 328 с.
4. Бормотов СВ. Системное администрирование на 100 % (+CD). — СПб.: Питер, 2006. — 256 с.
5. Варфоломеев А.А., Жуков А.Е., Пудовкина М.А. Поточные криптосистемы. Основные свойства и методы анализа стойкости. — М.: ПАИМС, 2000. — 36 с.
6. Жельников В. Криптография от папируса до компьютера. — М.: ABF, 1996. — 130 с.
7. Зубов А.Ю. Совершенные шифры. — М.: Гелиос АРВ, 2003. — 160 с.
8. Касперски К. Восстановление данных. Практическое руководство: Пер. с англ. — СПб.: БХВ-Петербург, 2006. — 352 с.
9. Касперски К., Рокко Е. Искусство дизассемблирования. Наиболее полное руководство в подлиннике. — СПб: БХВ-Петербург, 2008. — 891 с.
10. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. — М.: Издательская группа "БДЦ-пресс", 2006. — 304 с.
11. Митник К. Искусство вторжения: Пер. с англ. Семенова А.В. — М.: АйТи, ДМК Пресс, 2005. —280 с.
12. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. — СПб.: Лань, 2000. — 256 с.
13. Нечаев В.И. Элементы криптографии (Основы теории защиты информации). — М.: Высшая школа, 1999. — 200 с.

14. Низамутдинов М.Ф. Тактика защиты н нападения на Web-приложения. — СПб.: БХВ-Петербург, 2005. — 432 с.
15. Норткат С, Новак Дж. Обнаружение нарушений безопасности в сетях. — М.: Издательский дом "Вильяме", 2003. — 448 с.
16. Оглтри Т. Firewalls. Практическое применение межсетевых экранов. — М. ДМК пресс, 2001. —400 с.
17. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. — М: ДМК, 2000. — 448 с.
18. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студ. высш. учеб. заведений / В.В. Платонов. — М. : Издательский центр "Академия", 2006. — 240 с.
19. Практическая криптографія: алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади. — М.: СОЛОН-Пресс, 2002. — 256 с.
20. Скляров Д. Искусство защиты и взлома информации. — СПБ.: БХВ-Петербург, 2004. — 288 с.
21. Смалько О.А. Захист інформаційних ресурсів: Монографія. - Кам'янець-Подільський: ПП Буйницький О А, 2011. - 704 с
22. Фленов М.Е. PHP глазами хакера. — СПб.: БХВ-Петербург, 2005. — 304 с.
23. Форд Дж. Ли. Персональная защита от хакеров. Руководство для начинающих. Пер. с англ. — М.: КУДИЦ-ОБРАЗ, 2002. – 272 с.
24. Фостер Дж., Лю В. Разработка средств безопасности и эксплойтов. – М.: Издательство "Русская Редакция"; СПб.: Питер, 2007. – 432 с.
25. Хоффман Л.Дж. Современные методы защиты информации. – М.: Сов. Радио, 1980. — 246 с.
26. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. – СПб.: Питер, 2003. – 368 с.
27. Щербаков Л.Ю., Домашев А.В. Прикладная криптография. Использование и синтез криптографических интерфейсов. – М: Издательско-торговый дом "Русская Редакция", 2003. – 416 с.

Додаткова:

28. Громов В.И. Васильев Г.А. Энциклопедия компьютерной безопасности. — Режим доступа: http://kiev-security.org.ua/b/1.shtml. —Название с экрана.
29. Зиммерман Филипп. Кодирование с открытым ключом для всех. Руководство пользователя PGP. — Режим доступа:

http://lib.metromir.ru/book2571. — Название с экрана.
30. Иллюстрированный самоучитель по защите информации. — Режим доступа: http://www.inattack.ru/program/525.html. — Название с экрана.
31. Иллюстрированный самоучитель по теории операционных систем. — Режим доступа: http://www.soft-info.ru/downloads/1230999291. — Название с экрана.
32. Руководство по информационной безопасности. — Режим доступа: http://unix1.jinr.ru/ faq_guide/security/jet/secplant. — Название с экрана.
33. Стандарты и спецификации в области информационной безопасности. Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт. Режим доступа: http://www.intuit.ru/department/security/secbasics/5. — Название с экрана.
34. Техника восстановления данных с лазерных дисков или практическое знакомство с сессиями. — Режим доступа: http://hack-tools.ucoz.com. — Название с экрана.
35. Ферри Д. Секреты супер-хакера. — Режим доступа: http://www.domknig.net/book-2697.html. — Название с экрана.

Інформаційні ресурси:

36. http://www.moodle.fi.npu.edu.ua/course/view.php?id=424.
37. http://www.moodle.fi.npu.edu.ua/course/view.php?id=425.

4. Форма підсумкового контролю успішності навчання

Екзамен є формою підсумкового контролю результатів навчання студентів і має на меті перевірку системності засвоєння програмового матеріалу, цілісності бачення навчального курсу, рівня осмислення знань та набуття умінь, їх комплексного застосування у практичній діяльності, діагностування ефективності самостійної навчальної роботи студентів.

Для запобігання репродуктивного характеру перевірки знань та умінь при проведенні екзамену передбачається використання теоретичних запитань, практичних і творчих завдань з метою виявлення можливих рівнів засвоєння студентами змісту навчального курсу.

Допуск до екзамену надається студенту при умові набору

більше 60 рейтингових балів і складанні всіх лабораторних робіт.

Якщо студент з поважних причин, що підтверджено документально, був відсутній на заняттях, він має право на одне перескладання з можливістю отримання максимальної кількості балів. Термін перескладання визначається викладачем.

Якщо впродовж семестру студент пропустив значну кількість занять, не має оцінок за виконання модулів, у відповідних графах «Відомості обліку успішності КМСОНП» виставляються „0”, у графі «екзамен» – відмітка про не допуск до нього.

Рейтинговий регламент Факультету. Шкала відповідності

За шкалою ECTS	**За шкалою університету**	**Визначення**	**Оцінка за національною шкалою**	
			Екзамен	**Залік**
A	90 – 100	Відмінно	5 (відмінно)	Зараховано
B	80 – 89	Дуже добре	4 (добре)	
C	70 – 79	Добре		
D	65 – 69	Задовільно	3 (задовільно)	
E	60 – 64	Достатньо		
FX	35 – 59	Незадовільно з можливістю повторного складання	2 (незадовільно)	Не зараховано
F	1 – 34	Незадовільно з обов’язковим повторним курсом		

5. Засоби діагностики успішності навчання

Видом контролю навчальних досягнень студентів під час вивчення курсу є залік або екзамен. За результатами роботи на лабораторних заняттях, виконання завдань для самостійного опрацювання, підготовки та виступу з доповіддю на заняттях, модульних тестів, студенти накопичують певну кількість балів, відповідно до якої відбувається оцінювання їх навчальних досягнень.

Залік є формою підсумкового контролю результатів навчання студентів і має на меті перевірку системності засвоєння програмового матеріалу, цілісності бачення навчального курсу, рівня осмислення знань та набуття умінь, їх комплексного застосування у практичній

діяльності, діагностування ефективності самостійної навчальної роботи студентів.

Відмітка «зараховано» виставляється студенту за умови набору більше 60 рейтингових балів, а саме:

- регулярного відвідування лекційних і лабораторних занять або їх негайного відпрацювання, своєчасного складання усіх видів поточного контролю з позитивними результатами;
- поглибленні набутих знань у процесі самостійної роботи;
- засвоєнні змісту навчального курсу в обсязі, передбаченому галузевим стандартом вищої освіти.

Побудова програми за блочно-модульною схемою спрямована на максимальну індивідуалізацію процесу навчання. Структура програми дібрана так, щоб надати студентам можливість навчатись в індивідуальному темпі та орієнтуватись на певні рівні вимог щодо засвоєння навчального матеріалу.

Контроль знань студентів здійснюється за модульно-рейтинговою системою. Навчальна діяльність студентів протягом семестру оцінюються за 100-бальною системою. Робота в семестрі поділяється на змістові модулі.

Накопичення балів протягом семестру відбувається так:

№ з/п	**Вид діяльності**	**Кількість балів за дидактичну одиницю**	**Кількість лекцій, практичних робіт тощо**	**Загальна кількість балів**
1	Виконання завдань на лабораторних заняттях	*10*	*14+2*	*160*
2	Відвідування та активність під час лекцій	*5*	*10*	*50*
3	Індивідуальна робота та презентація власних досліджень (самостійна робота)	*8*	*4*	*32*
Загальна кількість балів (поточна успішність)				***242***
Формула переведення балів у бали за модульно-рейтинговою системою 100*А/242, де А – кількість набраних студентом балів				***100***
Екзамен				*100*
Оцінка за курс (середній бал)				***100***

Засоби діагностики успішності навчання:

- теоретичні запитання та практичні завдання до лабораторних робіт;
- комплекс тестових завдань для модульного (підсумкового) контролю рівня навчальних досягнень студентів;
- індивідуальні завдання студентам;
- комплексна контрольна робота.

Питання до екзамену:

1. Основні поняття з галузі захисту даних. Актуальність проблеми комп'ютерної безпеки, цілісність даних, конфіденційність даних, доступність даних.
2. Основні поняття з галузі захисту даних. Розголошення даних, витік даних, захист даних, порушенням режиму доступу, несанкціонований доступ, об'єкт злочину, блокування даних, модифікація даних, одержання захищуваних даних.
3. Основні поняття з галузі захисту даних. Фільтрація даних, канал витоку даних, помилка, прорахунок, вразливість інформаційної системи.
4. Основні поняття з галузі захисту даних. Види загроз, джерела загроз, контроль безпеки, види атак, вторгнення, політика безпеки, класифікація навмисних загроз безпеки комп'ютерних систем.
5. Засоби парольної ідентифікації та адміністрування. Ідентифікація, засоби парольної ідентифікації в операційних системах, в програмних додатках, в мережевих сервісах, способи захисту від перебирання паролів, варіанти заміни традиційних паролів, способи створення складних паролів.
6. Архівування та резервне копіювання даних. Стискування, архівація даних, архіватор, ступінь стискування, коефіцієнт стискування, методи стискування файлів, резервне копіювання, технології резервного копіювання.
7. Захист вмісту зовнішньої пам'яті. Перспективні розробки у сфері зберігання вмісту запам'ятовуючих пристроїв, технології захисту оптичних дисків від несанкціонованого копіювання.
8. Захист вмісту зовнішньої пам'яті. Діагностика та профілактика

жорстких магнітних дисків, технології захисту флеш-накопичувачів,

9. Захист вмісту зовнішньої пам'яті. Засоби відновлення пошкодженого і втраченого вмісту запам'ятовуючих пристроїв, гарантоване вилучення вмісту запам'ятовуючих пристроїв.
10. Захист програмного забезпечення. Вразливості програмного забезпечення та засоби боротьби з ними, дослідження вихідних текстів програмного забезпечення.
11. Захист програмного забезпечення. Захист програм встановлених на жорсткому диску, захист програм від вивчення.
12. Захист вмісту запам'ятовуючих пристроїв від шкідливих програм. Комп'ютерні віруси і засоби боротьби з ними, історія комп'ютерних вірусів, класифікація комп’ютерних вірусів, антивірусні програми, типи антивірусних програм.
13. Захист вмісту запам'ятовуючих пристроїв від шкідливих програм. Методи розпізнавання шкідливих об'єктів, захист комп'ютера від шпигунських програм.
14. Поширені види мережевих атак і способи захисту від них. Сегментація мереж, міжмережеві екрани, списки управління доступом (ACL).
15. Поширені види мережевих атак і способи захисту від них. Загрози використання глобальної мережі Інтернет, методи захисту.
16. Організація бездротового зв'язку, специфічні атаки на бездротові мережі та способи захисту від них.
17. Актуальні проблеми використання безпровідних мереж, типи загроз безпеці в безпровідних мережах, способи захисту даних в безпровідних мережах.
18. Основні поняття криптографії. Поняття криптології, криптографії. Ключ, шифрування, зашифровування, розшифровування.
19. Основні поняття криптографії. Криптостійкість, криптоаналіз, методи криптоаналізу, криптографічні методи захисту даних.
20. Популярні алгоритми шифрування даних. Алгоритми шифрування, симетричні криптографічні алгоритми.
21. Популярні алгоритми шифрування даних. Алгоритми шифрування, асиметричні криптографічні алгоритми.
22. Криптосистеми з відкритим ключем, електронний (цифровий) підпис, Технології застосування систем електронного цифрового

підпису, генерація ключів.

23. Програмно-апаратні засоби шифрування даних. Реалізації криптозахисту на апаратному рівні. Архітектура апаратних засобів криптозахисту. Організація інтерфейсу для роботи з прикладними програмами.
24. Основні поняття стеганографії, історія стеганографії, стеганографічні методи і системи.
25. Проблеми шифрування великих повідомлень, сучасні способи вирішення проблеми розподілу ключів, системи біометричної аутентифікації, перспективи використання криптографічних засобів захисту даних.

Екзамен проводиться у формі комп'ютерного тестування, де потрібно відповісти на 62 тестових завдання, з яких 60 – це тестові завдання закритої форми (див.Рис. 1) та 2 (питання з білетів) тестових завдання відкритої форми (див.Рис. 2).

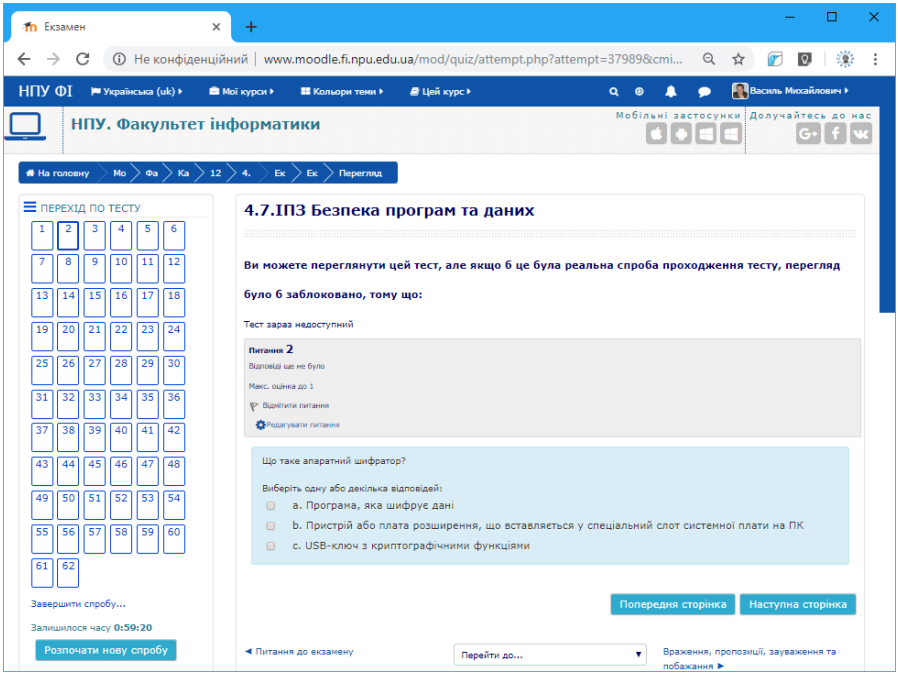

Рис. 1. Тестове завдання закритої форми

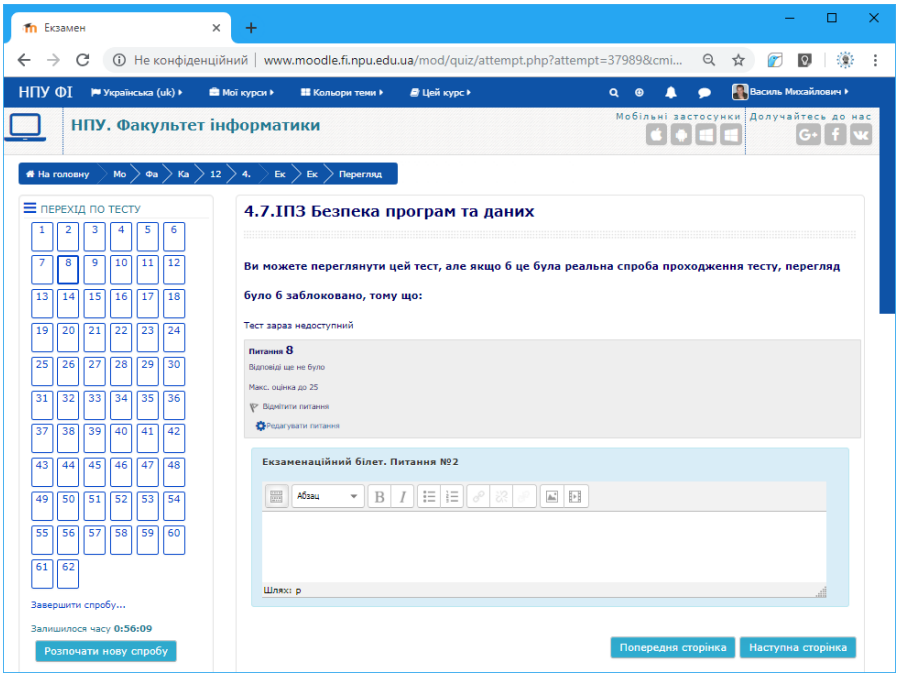

Рис. 2. Тестове завдання відкритої форми

ДЛЯ ЗАМІТОК