**МІНІСТЕРСТВО ОСВІТИ І НАУКИ,
МОЛОДІ ТА СПОРТУ УКРАЇНИ**

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

**Робоча програма
навчальної дисципліни**

"ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ"

**для студентів напряму підготовки
6.050101 "Комп'ютерні науки"
всіх форм навчання**

Харків. Вид. ХНЕУ, 2012

Затверджено на засіданні кафедри інформаційних систем.
Протокол № 2 від 14.09.2011 р.

Укладачі: Кузнецов О. О.
Євсеєв С. П.
Поляков А. О.
Король О. Г.

Р58 Робоча програма навчальної дисципліни "Технології захисту інформації" для студентів напряму підготовки 6.050101 "Комп'ютерні науки" всіх форм навчання / укл. О. О. Кузнецов, С. П. Євсеєв, А. О. Поляков та ін. – Х. : Вид. ХНЕУ, 2012. – 52 с. (Укр. мов.)

Подано тематичний план навчальної дисципліни та її зміст за модулями й темами, вміщено плани лабораторних робіт, розглянуто основні моменти, які допоможуть студентові при вивченні навчальної дисципліни.

Рекомендовано для студентів напряму підготовки 6.050101 "Комп'ютерні науки" всіх форм навчання.

Вступ

Навчальну дисципліну "Технології захисту інформації" зараховано до циклу професійної та практичної підготовки бакалаврів з напряму підготовки 6.050101 "Комп'ютерні науки". Вона є невід'ємною частиною циклу професійно-орієнтованої підготовки, необхідної працівникам підприємств незалежно від форми власності та організаційно-правової форми господарювання.

Основною метою викладання дисципліни є навчання студентів принципам побудови комплексних систем захисту інформації, розробки, дослідженню та застосуванню механізмів захисту інформації, що засновані на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення автентичності, цілісності та конфіденційності інформаційних систем та технологій (ІС та Т), вивчення студентами основ стеганографічного захисту інформації та особливості побудови інфраструктури відкритих ключів (ІВК).

Теоретичною базою вивчення навчальної дисципліни є такі дисципліни: "Вища математика", "Математичне програмування", "Інформатика та комп'ютерна техніка", теорія інформації, теорія ймовірностей і математичної статистики та теорія чисел.

Засобами досягнення мети та рішення завдань дисципліни є:

1. Підручники, навчально-методичні та довідкові посібники, технічна документація, що видані центральними видавництвами, а також розроблені на кафедрі інформаційних систем та видані у ХНЕУ.

2. Навчально-матеріальна база, до складу якої входять: обчислювальний центр з комплексом мережного обладнання, персональні комп'ютери, автоматизовані навчаючі системи, комплект дидактичних матеріалів, що складається зі слайдів, технічна апаратура.

Структура навчальної дисципліни наведена в табл. 1.

Форми проведення занять: лекції, лабораторні заняття.

Форми контролю:

поточний контроль – у формі тесту за модулями, у формі захисту лабораторних робіт;

підсумковий контроль – письмовий іспит у формі завдань з теорії та практики.

підсумкова оцінка складається з результату іспиту та поточного контролю.

Таблиця 1

Структура навчальної дисципліни

<table>
<tr><td>Навчальна дисципліна:
підготовка бакалаврів</td><td>Галузь знань, спеціалізація, освітньо-кваліфікаційний рівень</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Кількість кредитів відповідних ECTS: 4 кредити, у тому числі:
змістовних модулів – 2,
самостійна робота;
завдання для самостійної роботи</td><td>Шифр та назва галузі знань:
0501 "Інформатика та комп’ютерна техніка"
Шифр та назва напряму підготовки
6.050101 "Комп’ютерні науки"</td><td>Обов’язкова.

Рік підготовки: 4.

Семестр: 8</td></tr>
<tr><td>Загальна кількість годин – 144;
за змістовними модулями:
модуль 1 – 77;
модуль 2 – 77</td><td rowspan="2">Освітньо-кваліфікаційний рівень
бакалавр</td><td>Лекції (теоретична підготовка): 18 годин.

Лабораторні роботи: 36 годин.
Самостійна робота: 90 годин</td></tr>
<tr><td>Кількість тижнів викладання – 9.
Кількість годин за тиждень – 6</td><td>Вид контролю:
іспит</td></tr>
</table>

Необхідним елементом успішного засвоєння навчального матеріалу дисципліни є самостійна робота студентів з літературою з питань вивчення методів та алгоритмів криптографічного перетворення інформації механізмів та протоколів забезпечення захисту.

Самостійна робота студента повинна бути спрямована на якісну підготовку до лабораторних занять, на самостійне розв’язання завдань з тем лабораторних занять, що відбулися, з метою закріплення практичних і методичних навичок з дисципліни. Перед плановими лабораторними заняттями викладач видає конкретне завдання до підготовки до нього з зазначенням теми, мети, питань, що вивчаються, та рекомендованої літератури.

Час, що відводиться на самостійну підготовку з дисципліни, повинен використовуватись студентом для поглибленого вивчення теоретичного матеріалу дисципліни з використанням основної та додаткової літератури, що рекомендована на лекціях. Для цього викладач повинен наприкінці кожної лекції ставити конкретні завдання для самопідготовки з переліком питань, що вивчаються самостійно, та конкретних цілей, досягненню яких слугує їх обробка. При цьому цілі повинні бути щільно пов’язані з практичними завданнями підготовки студента як фахівця.

1. Кваліфікаційні вимоги до студентів у галузі захисту інформації в інформаційних системах

Навчальна дисципліна є обов'язковою для підготовки бакалаврів напряму підготовки "Комп'ютерні науки".

Необхідна навчальна база перед початком вивчення дисципліни: з метою кращого засвоєння навчального матеріалу дисципліни студенти повинні до його початку опанувати знаннями та навичками в області дискретної математики, комп'ютерної техніки, фахових навчальних дисциплін – "Алгоритмізація та програмування", "Комп'ютерна схемотехніка та архітектура комп'ютерів". У свою чергу знання з даної дисципліни забезпечують успішне виконання курсових і дипломних проектів.

Після вивчення даної дисципліни студенти повинні

***знати*:**

основні положення законодавства в галузі захисту інформації, основні міжнародні та національні стандарти з безпеки ІС та Т;

основні терміни та визначення політики безпеки, принципи побудови профілю захисту інформації для забезпечення послуг безпеки;

механізми та протоколи забезпечення конфіденціальності ІС та Т;

механізми та протоколи забезпечення автентичності ІС та Т;

механізми та протоколи забезпечення цілісності даних ІС та Т;

модель порушника, основні види атак, принципи криптоаналізу;

механізми та протоколи керування ключами в ІВК інформаційної системи;

методи та процедури цифрової стеганографії.

***отримати такі компетенції*:**

здатність визначати вимоги політики безпеки та формувати профіль захисту відповідно до забезпечення послуг безпеки в ІС та Т;

здатність ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів та протоколів захисту інформації в ІС та Т;

здатність забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації;

здатність аналізувати технічні параметри діючих протоколів та механізмів захисту інформації з точки зору використання в комп'ютерних системах та мережах, впливу їх характеристик на основні показники ІС та Т в цілому;

здатність проводити аналіз ефективності прийнятих технічних рішень щодо забезпечення захисту інформації в інформаційних системах, користуватися математичним та статистичним апаратом щодо вирішення інженерних завдань, які виникають під час розробки та дослідження механізмів;

здатність забезпечувати захист програмного та інформаційного забезпечення від несанкціонованих дій;

здатність здійснювати захист даних в корпоративних розподілених інформаційних системах, застосовувати системи криптографії в професійній діяльності.

Програму навчальної дисципліни розроблено у відповідності до вимог галузевого стандарту вищої освіти на базі освітньо-професійної програми підготовки бакалавра. Враховано рекомендації положень Болонської декларації щодо кредитно-модульної системи організації навчального процесу. Програма навчальної дисципліни відповідає вимогам Галузевого стандарту вищої освіти України з напряму підготовки 6.050101 "Комп'ютерні науки".

2. Тематичний план навчальної дисципліни

При вивченні навчальної дисципліни студент має ознайомитися з програмою дисципліни, її структурою, формами та методами навчання, видами та методами контролю знань. Тематичний план дисципліни складається з двох модулів, які охоплюють основні положення та механізми захисту інформації в інформаційних системах.

Навчальний процес здійснюється у таких формах: лекційні та лабораторні заняття, самостійна робота студента. Структура залікового кредиту дисципліни наведена в табл. 2.

Таблиця 2

Структура залікового кредиту навчальної дисципліни

Тема	Кількість годин, відведених на:		
	лекції	лабораторні заняття	самостійну роботу
1	2	3	4
Змістовний модуль 1. Безпека і захист даних			
Тема 1. Огляд безпеки системи	1		2
Тема 2. Механізми і політики розмежування прав доступу	1		8

Закінчення табл. 2

1	2	3	4
	1		8
Тема 3. Методи та пристрої забезпечення захисту і безпеки	1		4
Тема 4. Захист, доступ та автентифікація	1		10
Тема 5. Моделі захисту. Захист пам'яті	1		6
Тема 6. Шифрування даних	1	14	10
Тема 7. Управління відновленням	1		4
Тема 8. Основні напрями розвитку сучасної криптографії	1	6	4
Тема 9. Механізми та протоколи керування ключами в ІВК інформаційної системи	2	4	8
Змістовний модуль 2. Мережева безпека			
Тема 10. Основні види атак, принципи криптоаналізу. Основи криптографії	2	4	10
Тема 11. Алгоритми з секретним ключем	1		4
Тема 12. Алгоритми з відкритим ключем	1	4	8
Тема 13. Протоколи автентифікації	1		4
Тема 14. Цифрові підписи	1	4	4
Тема 15. Використання паролів і механізмів контролю за доступом	2		4
Всього	18	36	90

3. Зміст дисципліни за модулями та темами

Змістовний модуль 1. Безпека і захист даних

Тема 1. Огляд безпеки системи

Основні поняття та визначення безпеки. Роль захисту інформації в ІС, умови функціонування підсистеми безпеки в комп'ютерних мережах та системах. Вимоги щодо безпеки системи, ризики безпеки. Послуги безпеки: конфіденційність, цілісність, автентичність, причетність, спостереженість. Розподіл послуг безпеки за рівнями моделі ISO/OSI. Критерії

захищеності комп'ютерних систем. Розробка профілю захисту. Механізми реалізації послуг безпеки. Стандарт ISO-7498-2. Побудування та впровадження систем захисту інформації.

Тема 2. Механізми і політики розмежування прав доступу

Засоби забезпечення захисту інформації в СУБД. Засоби ідентифікації й автентифікації об'єктів баз даних, управління доступом. Засобу контролю цілісності інформації, організація аудиту. Скасування прав доступу. Видача прав доступу до об'єктів баз даних.

Тема 3. Методи та пристрої забезпечення захисту і безпеки

Компоненти криптосистеми та їх функціональні характеристики. Побудова класифікацій криптографічних засобів. Захист інформації за допомогою міжмережних екранів.

Тема 4. Захист, доступ та автентифікація

Загальні механізми забезпечення безпеки. Взаємозв'язок послуг та механізмів безпеки і взаємозв'язок послуг і рівнів моделі взаємодії відкритих систем. Автентифікація даних, механізми забезпечення та методи автентифікації.

Тема 5. Моделі захисту. Захист пам'яті

Побудова моделі порушника безпеки. Організація захисту, захист окремих чарунок пам'яті. Основні засоби захисту пам'яті при керуванні та з привілеями. Моделі безпеки, які застосовуються при побудові захисту в СУБД. Захист БД в системах з видаленим доступом. Інтерфейси CGI, API й FastCGI.

Тема 6. Шифрування даних

Математичні основи сучасної теорії захисту інформації. Методи булевої алгебри, елементи кореляційного та спектрального аналізу. Прості шифри. Симетричне шифрування даних. Криптографічні примітиви й типи структур симетричного шифрування. Блочні симетричні шифри, алгоритми блокового симетричного шифрування DES, ГОСТ-28147, Rijndael. Архітектура блочних симетричних шифрів. Типові режими роботи криптосистеми: "Електронна кодова книга", "Зчеплення блоків

шифру", "Зворотний зв’язок з шифру", "Зворотний зв’язок з виходу". Режим простої заміни. Режим гама шифрування. Режим шифрування зі зворотним зв’язком за виходом. Режим вироблення імітовставки. Потокові шифри. Регістри зсуву зі зворотнім зв’язком. Асиметричне шифрування даних. Математичні положення теорії скінченних полів та систем класів лишків. Математичні положення теорії чисел. Асиметричні алгоритми шифрування даних RSA та Ель Гамаля.

Тема 7. Управління відновленням

Захист і відновлення даних. Формування служб резервного копіювання й відновлення даних для критично-важливих серверів. Кластерізація серверів. Етапи управління формуванням плану резервного відновлення. Типи та топології резервного копіювання.

Тема 8. Основні напрями розвитку сучасної криптографії

Основні криптографічні примітиви. Математичні моделі нелінійних вузлів замін у термінах булевої алгебри. Основні напрями розвитку асиметричних криптоалгоритмів. Криптографія на еліптичних кривих. Теоретико-чисельні задачі, складність арифметики точок ЕК в різних формах і представленнях. Цифрова стеганографія з відкритим ключем.

Тема 9. Механізми та протоколи керування ключами в ІВК інформаційної системи

Компоненти та сервіси інфраструктури відкритих ключів. Архітектура і топологія PKI. Стандарти в галузі PKI. Сертифікати відкритих ключів X.509, управління сертифікатами. Системи PKI. Документ політика захисту інформації, його сутність та структура, управління ключами. Профілі безпеки автоматизованих систем. Основні вимоги до політиці PKI.

Змістовний модуль 2. Мережева безпека

Тема 10. Основні види атак, принципи криптоаналізу. Основи криптографії

Формальне математичне визначення криптосистеми. Критерії та показники ефективності. Аналіз основних видів атак, рисків та вразливих елементів інформаційних систем. Класифікація криптоаналітичних атак.

Диференціальний криптоаналіз, диференціальний криптоаналіз на основі відмов пристрою. Лінійний криптоаналіз. Силова атака на основі розподілених розв'язань.

Тема 11. Алгоритми з секретним ключем

Захист інформації на мережному рівні. Протоколи захисту та цілісності IPSec, SSL, TLS, їх сутність.

Тема 12. Алгоритми з відкритим ключем

Системи захисту PGP та CS MIME. Криптографічні функції. Сумісність на рівні електронної пошти. Захищена електронна пошта.

Тема 13. Протоколи автентифікації

Класифікація механізмів автентифікації. MDC-коди, основні алгоритми. MAC-коди, основні способи формування. Методи побудови універсальних геш-функцій.

Тема 14. Цифрові підписи

Класифікація стандартів електронних цифрових підписів. Моделі цифрових підписів. Основні стандарти цифрового підпису.

Тема 15. Використання паролів і механізмів контролю за доступом

Основні принципи захисту інформації при підключенні до мережі Інтернет. Використання паролів і механізмів контролю.

4. Плани лекцій

Змістовний модуль 1. Безпека і захист даних

Тема 1. Огляд безпеки системи

1.1. Завдання дисципліни. Структура та зміст дисципліни, її зв'язок з іншими дисциплінами.

1.2. Основні поняття та визначення безпеки. Роль захисту інформації в ІС, умови функціонування підсистеми безпеки в комп'ютерних мережах та системах. Вимоги щодо безпеки системи, ризики безпеки.

1.3. Послуги безпеки: конфіденційність, цілісність, автентичність, причетність, спостереженість. Розподіл послуг безпеки за рівнями моделі ISO/OSI. Критерії захищеності комп'ютерних систем.

1.4. Розробка профілю захисту. Механізми реалізації послуг безпеки. Стандарт ISO-7498-2.

Література: [1; 2; 7 – 9; 12 – 17].

Тема 2. Механізми і політики розмежування прав доступу
Тема 3. Методи та пристрої забезпечення захисту і безпеки

2.1. Засоби забезпечення захисту інформації в СУБД. Засоби ідентифікації й автентифікації об'єктів баз даних, управління доступом. Засоби контролю цілісності інформації, організація аудиту.

2.2. Компоненти криптосистеми та їх функціональні характеристики.

2.3. Побудова класифікацій криптографічних засобів.

2.4. Захист інформації за допомогою міжмережних екранів.

Література: [11 – 14].

Тема 4. Захист, доступ та автентифікація
Тема 5. Моделі захисту. Захист пам'яті

3.1. Загальні механізми забезпечення безпеки. Взаємозв'язок послуг та механізмів безпеки і взаємозв'язок послуг і рівнів моделі взаємодії відкритих систем.

3.2. Автентифікація даних, механізми забезпечення та методи автентифікації.

3.3. Побудова моделі порушника безпеки. Організація захисту, захист окремих чарунок пам'яті. Основні засоби захисту пам'яті при керуванні та з привілеями.

3.4. Моделі безпеки, які застосовуються при побудові захисту в СУБД. Захист БД в системах з видаленим доступом.

Література: [13 – 15].

Тема 6. Шифрування даних

4.1. Математичні основи сучасної теорії захисту інформації. Методи булевої алгебри, елементи кореляційного та спектрального аналізу.

4.2. Симетричне шифрування даних. Криптографічні примітиви й типи структур симетричного шифрування.

4.3. Блочні симетричні шифри, алгоритми блокового симетричного шифрування DES, ГОСТ-28147, Rijndael.

4.4. Потокові шифри. Регістри зсуву зі зворотнім зв'язком.

Література: [12; 13; 16].

Тема 7. Управління відновленням

5.1. Асиметричне шифрування даних.

5.2. Математичні положення теорії чисел.

5.3. Асиметричні алгоритми шифрування даних RSA та Ель Гамаля.

5.4. Захист і відновлення даних. Етапи управління формуванням плану резервного відновлення. Типи та топології резервного копіювання.

Література: [3; 7 – 9; 11 – 13; 16].

Тема 8. Основні напрями розвитку сучасної криптографії

6.1. Основні криптографічні примітиви. Математичні моделі нелінійних вузлів замін у термінах булевої алгебри.

6.2. Основні напрями розвитку асиметричних криптоалгоритмів. Криптографія на еліптичних кривих.

6.3. Теоретико-чисельні задачі, складність арифметики точок ЕК в різних формах і представленнях.

6.4. Цифрова стеганографія з відкритим ключем.

Література: [5; 6; 8].

Тема 9. Механізми та протоколи керування ключами в ІВК інформаційної системи

7.1. Компоненти та сервіси інфраструктури відкритих ключів. Архітектура і топологія PKI.

7.2. Стандарти в галузі PKI. Сертифікати відкритих ключів X.509, управління сертифікатами.

7.3. Системи PKI. Документ політика захисту інформації, його сутність та структура, управління ключами.

7.4. Профілі безпеки автоматизованих систем. Основні вимоги до політиці PKI.

Література: [4; 8; 15].

Змістовний модуль 2. Мережева безпека

Тема 10. Основні види атак, принципи криптоаналізу. Основи криптографії
Тема 11. Алгоритми з секретним ключем
Тема 12. Алгоритми з відкритим ключем

8.1. Формальне математичне визначення криптосистеми. Критерії та показники ефективності. Аналіз основних видів атак, ризиків та вразливих елементів інформаційних систем. Класифікація криптоаналітичних атак.

8.2. Диференціальний криптоаналіз, диференціальний криптоаналіз на основі відмов пристрою. Лінійний криптоаналіз.

8.3. Захист інформації на мережному рівні. Протоколи захисту та цілісності IPSec, SSL, TLS, їх сутність.

8.4. Системи захисту PGP та CS MIME.

Література: [2; 7; 8; 11 – 15; 18].

Тема 13. Протоколи автентифікації
Тема 14. Цифрові підписи
Тема 15. Використання паролів і механізмів контролю за доступом

9.1. Класифікація механізмів автентифікації. MDC-коди, основні алгоритми. MAC-коди, основні способи формування.

9.2. Класифікація стандартів електронних цифрових підписів. Основні стандарти цифрового підпису.

9.3. Основні принципи захисту інформації при підключенні до мережі Інтернет.

9.4. Використання паролів і механізмів контролю.

Література: [8; 12 – 14; 16].

5. Плани лабораторних занять

Лабораторні заняття – це організаційна форма навчального заняття, на якому студент під керівництвом викладача особисто проводить натурні або імітаційні експерименти чи досліди з метою практичного підтвердження окремих теоретичних положень даної навчальної дисципліни, набуває практичних навичок роботи з лабораторним устаткуванням, обладнанням, обчислювальною технікою, вимірювальною апаратурою, методикою експериментальних досліджень у конкретній предметній галузі.

Лабораторне заняття проводиться з студентами, кількість яких не перевищує половини академічної групи.

Лабораторне заняття включає проведення поточного контролю підготовленості студентів до виконання конкретної лабораторної роботи, виконання завдань теми заняття, оформлення індивідуального звіту з виконаної роботи та його захист перед викладачем.

На лабораторних заняттях особлива увага приділяється прикладній спрямованості матеріалу з метою вироблення у студентів навичок самостійного інженерного мислення, вміння вирішувати завдання аналізу та синтезу основних пристроїв та ПК в цілому, та алгоритмів їх функціонування.

На лабораторних заняттях студенти самостійно практично навчаються проводити аналіз механізмів й протоколів забезпечення захист інформації в ІС, що необхідно для засвоєння теоретичних знань та практичних засобів рішення типових завдань, котрі можуть вирішуватися ними в подальшої діяльності за спеціальністю.

У кінці кожного заняття студенту надаються рекомендації до самостійної роботи над темами дисципліни з метою поглибленого вивчення теоретичного матеріалу дисципліни з використанням основної та додаткової літератури, що рекомендована на лекціях. При цьому мета повинна бути щільно пов’язана з практичними завданнями підготовки студента як фахівця.

Лабораторні заняття слугують відбиттям принципів певних наукових шкіл, які склалися в університеті. У ході проведення їх відбувається активний процес формування фахівця, поглиблюються, поширюються і конкретизуються знання, одержані на лекціях і в ході самостійної роботи.

Оскільки лабораторні заняття проводяться у складі навчальної групи, яка об’єднує студентів з однаковою спеціальністю і спеціалізацією підготовки, на них вдається глибше пов’язати теорію з практикою у контексті майбутньої професійної діяльності фахівця і тим самим успішно реалізувати суб’єктно-діяльнісний підхід у навчанні.

Для успішної реалізації призначення і ролі лабораторних занять в структурі навчальної дисципліни і всього процесу навчання, їх підготовка і проведення повинні відповідати ряду вимог. Вимоги розподіляються на загальні до лабораторних занять і специфічні – для обмеженої групи або циклу дисциплін.

До *загальних вимог* зараховують:

1. Зміст лабораторного заняття повинний бути тісно пов'язаний з лекціями та самостійною роботою студентів. Лабораторне заняття повинно бути логічним розвитком лекції. Одночасно воно може готувати студентів до поміркованого виконання практичних робіт. На лабораторних заняттях допустимо і доцільно доповнювати знання студентів новою інформацією з часткових проблем і питань прикладного характеру.

Зміст і методика проведення заняття повинні розроблятися неодмінно за участю лектора та під його керівництвом. Необхідно, щоби лектор особисто проводив лабораторні заняття хоча б в одній навчальній групі, а викладачі, які проводять ці заняття, систематично відвідували лекції з дисципліни.

2. Лабораторне заняття повинно реалізовувати суб'єктно-діяльнісний (контекстний) підхід у навчанні, забезпечувати навчання в контексті з майбутньою професійною діяльністю випускників університету. Тому формулювання винесених на заняття проблемних питань та умови задач для кожної навчальної групи одного потоку можуть різнитися, у залежності від спеціальності (спеціалізації) підготовки студентів.

Лектор потоку і викладачі, які проводять лабораторні заняття, повинні знати зміст навчальних дисциплін, які вони забезпечують своєю дисципліною, а в багатьох випадках – принципи побудови, основи застосування механізмів і протоколів забезпечення захисту інформації в ІС за спеціальністю (спеціалізації) підготовки студентів.

3. Методика проведення лабораторного заняття і його зміст повинні опиратися на знання, які набуті студентами в результаті відпрацювання лекцій і рекомендованої літератури за темою заняття. На початку проведення заняття або в ході його рівень засвоєння цих знань контролюється викладачем. У разі необхідності викладач повинен корегувати, уточнювати та поглиблювати знання студентів.

4. Основу лабораторного заняття повинна складати індивідуальна самостійна робота студентів при керуючому впливі викладача у сполученні із колективним обговоренням проблемних питань, відпрацюванням шляхів і методики розв'язання поставлених завдань. Для підвищення ефективності індивідуальної роботи студентів, розвитку їх самостійності, доцільно передбачати і використати можливість соціальної стимуляції з боку товаришів навчальної групи, створюючи тим самим обстановку відповідальної залежності кожного від колективу.

Специфічні вимоги до лабораторних занять характеризуються таким чином.

Професійна спрямованість лабораторних занять *з природно-наукових дисциплін* повинна проявлятися, головним чином, у тому, щоб зміст кожного заняття був орієнтований на засвоєння студентами знань і набуття вмінь, необхідних для вивчення професійно-орієнтованих та спеціальних дисциплін зі спеціальності (спеціалізації).

При визначенні цільових настанов і змісту лабораторних занять *з професійно-орієнтованих дисциплін* поряд із забезпеченням внутрішніх потреб цих дисциплін, слід звертати особливу увагу на необхідність формування у студентів певних вмінь, які наведені в освітньо-кваліфікаційній характеристиці випускника університету і забезпечуються дисципліною, що вивчається. Передбачати також формування певних знань і вмінь, необхідних для освоєння відповідних спеціальних дисциплін. Зміст лабораторного заняття повинен визначатись диференційовано для кожної навчальної групи з урахуванням спеціальності (спеціалізації) підготовки студентів в групі та їх майбутньої професійної діяльності. Разом з тим, зміст повинен забезпечувати виконання загальних задач, які визначаються єдиним для всіх груп потоку напрямом підготовки.

При підготовці та проведенні лабораторних занять за *спеціальними дисциплінами* необхідно передбачати:

формування у студентів вмінь та знань, які відображаються не тільки в основній, але й у варіативній частинах освітньо-кваліфікаційної характеристики та освітньо-професійної програми;

використання методичних прийомів, які забезпечують єдність навчальної діяльності студентів з його майбутньою професіональною діяльністю;

планування занять у спеціалізованих класах (лабораторіях), які обладнані пристроями та відповідними елементами, програмними макетами, та іншими наочними приладами, а також засобами статичної та динамічної проекції.

Структура лабораторних занять може бути різноманітною в залежності від характеру дисциплін та курсу навчання. Тому стосовно структури можна дати тільки загальні рекомендації.

Кожне заняття повинно починатися зі вступу, у якому оголошується тема, цільова настанова і план проведення заняття. Визначається місце заняття у навчальному процесі, називаються питання, які повинні бути засвоєні студентами при підготовці до заняття.

В основній частині заняття колективне обговорення проблем, завдань і питань поєднується з індивідуальною практичною роботою студентів.

Виконання лабораторної роботи оцінюється викладачем. Підсумкова оцінка виставляється у журналі обліку виконання лабораторних робіт. Підсумкові оцінки, отримані студентом за виконання лабораторних робіт, враховуються при виставленні семестрової підсумкової оцінки з даної навчальної дисципліни. Підсумкові оцінки за кожне лабораторне заняття вносяться у відповідний журнал. Отримані студентом оцінки за окремі лабораторні заняття враховуються при визначенні поточної модульної оцінки з даної навчальної дисципліни (практичний модульний контроль). Перелік тем лабораторних занять наведений в табл. 3.

Таблиця 3

Перелік тем лабораторних занять

№з/п	Теми лабораторних занять	Кіль-кість годин
Змістовний модуль 1. Безпека і захист даних		
1	Класичні симетричні системи. Дослідження крипостійкості простих симетричних шифрів	2
2	Дослідження сучасних блочних симетричних шифрів та режимів шифрування	4
3	Система блокового шифрування S-DES. Дослідження розсіювальних властивостей S-DES	4
4	Дослідження сучасних асиметричних криптосистем шифрування. Стандарт ДСТУ ISO\IEC 15948-2	4
5	Дослідження інтегрованих механізмів забезпечення конфіденційності і вірогідності даних	4
6	Стеганографічні методи захисту інформації	2
7	Розгортання та управління інфраструктурою відкритих ключів	4
Змістовний модуль 2. Мережева безпека		
8	Статистичні дослідження генераторів випадкових та псевдовипадкових послідовностей за методикою NIST	4
9	Безпечність персональних конфіденціальних даних на базі секретного диску та захищеної електронної пошти PGP	4
10	Дослідження електронного цифрового підпису. ЦП Ель Гамаля, ДСТУ-4145, ECDSA	4

При виконанні ЛР студент повинен продемонструвати:

творчий підхід до дослідження тематики процедур та механізмів забезпечення захисту інформації в ІС;

грамотне використання програмного забезпечення макетів алгоритмів криптографічного перетворення інформації;

навички висококваліфікованого конфігурування і використання відповідних програмних засобів та додатків.

Студент повинен вміти правильно використовувати програмний макет процедур забезпечення захисту інформації, використовувати якісний аналіз отриманих параметрів і характеристик, виконувати оцінку отриманих результатів. Велике значення має графічне представлення отриманого матеріалу (у вигляді screensave-ів) з описом і поясненнями до використовуваного додатка.

Виконання лабораторних робіт містить такі етапи:

1. Підготовчий етап (до проведення ЛР):

а) одержання відповідного даним методичним вказівкам завдання, номера варіанту і вимог викладача;

б) вивчення теоретичного матеріалу за темою ЛР;

в) розробка алгоритму виконання завдання.

2. Безпосереднє виконання завдання у комп'ютерному класі обчислювального центру.

а) проходження допуску до ЛР;

б) установка (при необхідності), конфігурування додатка;

в) відпрацьовування завдання за варіантом;

г) аналіз отриманих параметрів і характеристик.

3. Виконання звіту і захист ЛР.

Звіт з лабораторної роботи повинен містити:

титульний лист із найменуванням ЛР і даними виконавця;

дату виконання;

особистий підпис;

мету роботи;

опис завдання;

опис алгоритму виконання завдання;

результати роботи і їх аналіз;

висновки з роботи.

Усі матеріали звіту необхідно зброшурувати, сторінки пронумерувати.

Звіт з ЛР згідно нормативним актам повинен захищатися виконавцем. Форму проведення захисту ЛР обирає викладач.

6. Самостійна робота студента

Необхідним елементом успішного засвоєння навчального матеріалу дисципліни є самостійна робота студентів з вітчизняною та закордонною спеціальною технічною літературою, стандартами з питань захисту інформації в інформаційних системах. Самостійна робота студента є основним засобом оволодіння навчальним матеріалом у час, вільний від обов'язкових навчальних занять.

Навчальний час, відведений для самостійної роботи студента, регламентується робочим навчальним планом і повинен становити не менше 1/3 та не більше 2/3 загального обсягу навчального часу студента, відведеного для вивчення конкретної дисципліни.

Зміст самостійної роботи студента над конкретною дисципліною визначається навчальною програмою дисципліни, методичними матеріалами, завданнями та вказівками викладача.

Самостійна робота студента забезпечується системою навчально-методичних засобів, передбачених для вивчення конкретної навчальної дисципліни: підручник, навчальні та методичні посібники, конспект лекцій викладача, практикум тощо.

Методичні матеріали для самостійної роботи студентів повинні передбачати можливість проведення самоконтролю з боку студента.

Для самостійної роботи студенту також рекомендується відповідна наукова та фахова монографічна і періодична література.

Самостійна робота студента над засвоєнням навчального матеріалу з конкретної дисципліни може виконуватися у бібліотеці вищого навчального закладу, навчальних кабінетах, комп'ютерних класах (лабораторіях), а також у домашніх умовах.

У необхідних випадках ця робота проводиться відповідно до заздалегідь складеного графіка, що гарантує можливість індивідуального доступу студента до потрібних дидактичних засобів.

Графік доводиться до відома студентів на початку поточного семестру.

При організації самостійної роботи студентів з використанням складного обладнання чи устаткування, складних систем доступу до інформації (наприклад, комп'ютерних баз даних, систем автоматизованого проектування тощо) передбачається можливість отримання необхідної консультації або допомоги з боку фахівця.

Навчальний матеріал навчальної дисципліни, передбачений робочим навчальним планом для засвоєння студентом в процесі самостійної роботи, виноситься на підсумковий контроль поряд з навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

Основні види самостійної роботи, які запропоновані студентам:

1. Вивчення лекційного матеріалу.
2. Робота з вивчення рекомендованої літератури.
3. Вивчення основних термінів та понять з галузі захисту інформації в ІС.
4. Підготовка до дискусій, роботи в малих групах.
5. Підготовка до підсумкового контролю.
6. Контрольна перевірка у кожного студента особистих знань за питаннями для самостійного поглибленого вивчення та самоконтролю.

Самостійна робота студентів проводиться з метою:

відпрацювання та засвоєння навчального матеріалу, закріплення та поглиблення знань, вмінь та навичок, що одержані на усіх видах навчальних занять;

виконання навчальних завдань, курсових, кваліфікаційних і дипломних робіт та проектів;

підготовки до майбутніх занять, заліків та екзаменів;

формування у студентів культури розумової праці, самостійності та ініціативи у пошуку та набутті знань.

Без систематичної, безперервної самостійної роботи студентів протягом всього періоду навчання неможливе засвоєння ними програмного матеріалу.

Самостійну роботу студентів забезпечують:

плануюча, організаційна і контролююча діяльність керівництва університету, навчального відділу, керівництва факультетів, кураторів;

методичне керівництво професорсько-викладацького складу;

організованість, дисциплінованість і сумлінне ставлення до навчання кожного студента;

наявність підручників і навчальних посібників з навчальних дисциплін, їх якість;

використання для самостійної роботи студентів обладнаних читальних залів, лабораторій, класів, спеціальних аудиторій;

рівномірний розподіл навчального навантаження на тиждень, місяць, семестр.

Відрив студентів від самостійної підготовки на заходи, не передбачені планами, категорично забороняється.

Планування самостійної роботи здійснюється кожним студентом.

6.1. Питання для самостійного опрацювання

Змістовний модуль 1. Безпека і захист даних

Тема 1. Огляд безпеки системи

Питання для самостійного поглибленого вивчення

1. "Жовтогаряча книга".
2. Критична та конфіденційна інформація.
3. Державна таємниця.
4. Інтелектуальна власність. Електроні документи.
5. Концепція архітектурних засобів безпеки ISO.
6. Послуги безпеки. Їх розподіл за моделлю ISO.
7. Політика безпеки.
8. Керування безпекою.
9. Функціональні вимоги безпеки.
10. Критерії адекватності систем безпеки.
11. Профіль захисту.

Теми доповідей

1. Життєвий цикл політики безпеки
2. Принципи побудови системи захисту інформації.
3. Проект профілю безпеки.

Література: основна [3; 5; 13; 15]; ресурси мережі Інтернет [26 – 28].

Тема 2. Механізми і політики розмежування прав доступу

Питання для самостійного поглибленого вивчення

1. Погрози подолання розмежувальною політики доступу до ресурсів.
2. Структура диспетчера доступу.
3. Вимоги до механізмів управління доступом.
4. Канонічна модель управління доступом.
5. Поняття та класифікація каналів взаємодії суб’єктів доступу.
6. Процедура авторизації.

Теми доповідей

1. Правила призначення міток безпеки ієрархічним об’єктам доступу.
2. Безпека доступу до коду в .NET.

3. Розмежування доступу процесів до системного диска в ОС Windows 7/ Server 2008 R2.

4. Розмежування доступу процесів до системного диска в ОС Unix та Linux.

Література: основна [2; 5; 13; 15]; ресурси мережі Інтернет [20; 26 – 28; 35].

Тема 3. Методи та пристрої забезпечення захисту і безпеки

Питання для самостійного поглибленого вивчення

1. Генератори випадкових чисел.
2. Біометричні пристрої автентифікації.
3. Криптопровайдери.
4. Мережні політики фільтрації трафіку.

Теми доповідей

1. Особливості міжмережного екранування на різних рівнях моделі OSI.
2. Архітектура сучасного міжмережного екрану.

Література: основна [3; 7; 13; 15; 17]; ресурси мережі Інтернет [29; 34; 35].

Тема 4. Захист, доступ та автентифікація

Питання для самостійного поглибленого вивчення

1. Автентифікація джерела даних та об’єкту комунікацій.
2. Конфіденційність з’єднання, трафіку, віддаленого поля даних.
3. Цілісність з’єднання з відновленням.
4. Обмін аутентичними ключами за допомогою асиметричної криптографії.

Теми доповідей

1. Протоколи автентифікації для забезпечення безпеки в мережі Інтернет.
2. Реалізація система автентифікації на основі служби каталогів.
3. Реалізація система автентифікації відкритих ключів без підтримки служби каталогів.

Література: основна [1; 3; 12; 14; 15]; ресурси мережі Інтернет [21; 28; 34].

Тема 5. Моделі захисту. Захист пам’яті

Питання для самостійного поглибленого вивчення

1. Розподіл пам’яті в операційних системах.
2. Прозоре шифрування даних.

3. Механізми захисту ключів.

4. Мандатна адресація.

Теми доповідей

1. Використання BitLocker для захисту персональних даних в OS Windows 7.

2. Використання PGP Disk для захисту персональних даних.

Література: основна [16]; ресурси мережі Інтернет [28; 35].

Тема 6. Шифрування даних

Питання для самостійного поглибленого вивчення

1. Механізми забезпечення конфіденціальності на основі сучасних симетричних алгоритмів шифрування.

2. Принципи блочного шифрування.

3. Поняття секретності системи шифрування. Досконала секретність.

4. Спрямоване шифрування.

5. Практичні способи використання режимів блочних шифрів.

6. Поточне шифрування. Алгоритми поточного шифрування.

7. Алгоритм Advanced Encryption Standard (AES, алгоритм Rijndael).

8. Схеми спрямованого шифрування на еліптичній кривій.

Теми доповідей

1. Шифрування конфіденційної інформації на флеш носіях.

2. Шифрування даних в сучасних протоколах передачі інформації.

Література: основна [2; 3; 7; 10; 14; 15]; ресурси мережі Інтернет [28; 35].

Тема 7. Управління відновленням

Питання для самостійного поглибленого вивчення

1. Повне видалення даних з носіїв інформації.

2. Механізми відновлення паролів в ОС.

3. Системи резервного копіювання дисків.

4. Журналізація змін.

Теми доповідей

1. План резервного відновлення БД після збою.

2. Методи відновлення БД після помилки обробки даних.

Література: основна [8; 11 – 14; 16]; ресурси мережі Інтернет [19; 20].

Тема 8. Основні напрями розвитку сучасної криптографії

Питання для самостійного поглибленого вивчення

1. Теорія чисел і криптографія.
2. Атаки на стеганографічні системи.
3. Зниження обчислювальної складності криптографічних перетворень.
4. Квантова криптографія.
5. Колективі криптографічні протоколи.

Теми доповідей

1. Огляд стеганоалгоритмів, що дозволяють вбудовувати інформацію у зображення.
2. Криптоаналіз на основі квантової криптографії.

Література: основна [8; 11 – 14; 16]; ресурси мережі Інтернет [28 – 30].

Тема 9. Механізми та протоколи керування ключами в ІВК інформаційної системи

Питання для самостійного поглибленого вивчення

1. Політика використання сертифікатів.
2. Сертифікати відкритих ключів X.509.
3. Компоненти і сервіси інфраструктури відкритих ключів.
4. Списки скасованих сертифікатів.
5. Політика ІВК.
6. Проблеми та ризики технології ІВК.

Теми доповідей

1. Розгортання інфраструктури відкритих ключів.
2. Програмні засоби підтримки PKI.

Література: основна [3; 12; 14; 18]; ресурси мережі Інтернет [28].

Змістовний модуль 2. Мережева безпека

Тема 10. Основні види атак, принципи криптоаналізу. Основи криптографії

Питання для самостійного поглибленого вивчення

1. Модель порушника.
2. Вимоги до сучасних криптоалгоритмів.

3. Факторизація. Метод факторізації загальне решето числового поля.

4. Методи розв'язання дискретний логарифму в групі точок еліптичній кривій.

Теми доповідей

1. Погрози та атаки проникнення в інформаційну систему.
2. Параметри крипто алгоритмів та складність криптоатак.

Література: основна [4; 14; 15], ресурси мережі Інтернет [28; 30].

Тема 11. Алгоритми з секретним ключем

Питання для самостійного поглибленого вивчення

1. Побудування VPN мереж.
2. Ключові та без ключові геш-функції.
3. Шифрування трауфіку в протоколі IPSec.
4. Шифрування трауфіку та забезпечення цілісності даних в протоколі SSL.
5. Шифрування трауфіку та забезпечення цілісності даних в протоколі TLS.

Теми доповідей

1. Захищеність VPN мереж.
2. Механізми забезпечення конфіденційності даних на прикладному рівні моделі OSI.

Література: основна [3; 7; 8; 14; 15; 17]; ресурси мережі Інтернет [28].

Тема 12. Алгоритми з відкритим ключем

Питання для самостійного поглибленого вивчення

1. Керування ключами в протоколі IPSec.
2. Перевірка дійсності сертифікатів.
3. Цілісність та автентичність в протоколах прикладного рівня моделі OSI.
4. Модель використання відкритих ключів в системі PGP.

Теми доповідей

1. Використання протоколу узгодження ключів в протоколах SSL та TLS.
2. Перевага асиметричної криптографії над симетричною.

Література: основна [2; 3; 4, 8; 11; 14; 18]; ресурси мережі Інтернет [28; 35].

Тема 13. Протоколи автентифікації

Питання для самостійного поглибленого вивчення

1. Механізми забезпечення автентичності на основі сучасних асиметричних процедур шифрування, MAC-кодів.
2. Сучасні алгоритми хешування.
3. Автентифікація повідомлень і геш-функція хешування.
4. Прості функції хешування. Захист функцій хешування.

Теми доповідей

1. Методи автентифікації віддаленого користувача в мережі Internet.
2. Протокол видаленої реєстрації SHH.

Література: основна [3; 7; 8; 14; 15]; ресурси мережі Інтернет [34; 35].

Тема 14. Цифрові підписи

Питання для самостійного поглибленого вивчення

1. Цифровий підпис з відновленням повідомлення.
2. Груповий цифровий підпис.
3. Сліпий цифровий підпис.
4. Разовий цифровий підпис.
5. Стандарти цифрового підпису на еліптичній кривій.

Теми доповідей

1. Юридичні аспекти використання цифрового підпису в Україні.
2. Європейські стандарти цифрового підпису, що гармонізовані в Україні.

Література: основна [3; 4; 6; 8 – 10; 14; 15]; ресурси мережі Інтернет [20; 28; 30].

Тема 15. Використання паролів і механізмів контролю за доступом

Питання для самостійного поглибленого вивчення

1. Протокол Нідхема і його реалізація в операційній системі UMIX.
2. Схема з одноразовими паролями.
4. Механізми реалізації дискреційної моделі доступу.
5. Механізми реалізації мандатної моделі доступу.
6. Реалізація пріоритетних розкладів в сучасних ОС.

Теми доповідей

1. Контроль за діями користувачів в ОС Windows 7/ Server 2008.
2. Контроль за діями користувачів в ОС UNIX та Linux.
3. Механізми контролю цілісності файлових об’єктів.

Література: основна [1; 14]; ресурси мережі Інтернет [20; 28; 35].

6.2. Тематика контрольних робіт для студентів заочної форми навчання

Контрольна робота є однією з форм контролю та обліку знань та вмінь студентів. Розрізняють контрольні роботи, які виконуються за семестровим розкладом занять, на заліках та екзаменах. Особливе місце належить контрольним роботам, які виконані студентами заочного навчання. Контрольна робота, являючись, в основному, засобом контролю, в той же час виконує навчальні та виховні функції. Контрольні роботи проводяться, як правило, у письмовій формі.

Контрольні роботи, які виконуються *за семестровим розкладом занять*, проводяться по дисциплінам згідно з навчальними планами та робочими навчальними програмами за рахунок часу, відведеного на вивчення дисципліни. Їх зміст може охоплювати найбільш важливі розділи (теми) навчальних дисциплін або увесь навчальний матеріал, який вивчений до її проведення. Студенти заочного навчання виконують контрольні роботи, як правило, в обсязі робочих навчальних програм дисциплін.

Зміст завдань визначається характером та обсягом навчального матеріалу, який виноситься на контрольну роботу, а також її цільовою настановою. Формулювання питань повинно вимагати від студентів не простого відтворення вивченого матеріалу на репродуктивному рівні, а спонукати до самостійності, проявленню творчої активності, узагальненням, встановленню зв’язку теорії з практикою. Завдання, як правило, повинні містить теоретичні та практичні питання, мати фронтальний характер у декількох варіантах. Вони можуть видаватись індивідуально кожному студенту. Це дозволяє залучати до перевірки великий за обсягом навчальний матеріал і, що особливо важливо, ураховувати різний рівень підготовки студентів. При такому варіюванню завдань контрольна робота дає найбільш повне та об’єктивне уявлення про знання та вміння студентів навчальної групи.

План проведення контрольної роботи, який містить її зміст, перелік дозволених до використання довідкових та інших матеріалів, опис методики проведення контрольної роботи, розглядається на засіданні предметно-методичної комісії та затверджується завідуючим кафедри.

Лектор потоку у вступній лекції з дисципліни поряд з іншими питаннями доводить до студентів необхідні відомості, які стосуються контрольної роботи, тим самим мобілізуючи їх на активну пізнавальну діяльність.

Перевірка результатів контрольної роботи та доведення оцінок по ній до студентів повинні здійснюватися у мінімальні строки. Чим більше відстрочений за часом аналіз результатів контрольної роботи, тим нижче її педагогічна ефективність, її значення для уточнення та поглиблення знань, для усунення виявлених недоліків.

Контрольні роботи можуть проводитись у формі виконання тестів з використанням електронної обчислювальної техніки.

Контрольна робота реферативного типу передбачає глибоке засвоєння студентами заочної форми навчання матеріалу навчальної дисципліни і включає п’ять практичних завдань, які потрібно пов’язати із практикою відпрацювання на мережі при її адмініструванні.

Усі завдання контрольної роботи повинні бути вирішенні. Індивідуальні варіанти обираються студентами відповідно до номеру в журналі.

Варіанти завдань до контрольних робіт

Завдання 1

Виконати шифрування та розшифрування свого прізвища, ім’я та по батькові за всіма методами шифрування, що наведені.

Провести оцінку криптографічної стійкості шифрів на основі порівняння множини ключів (кількості) K і множини одержуваних криптограм C. Завдання виконати відповідно до варіанта, що наведені нижче.

Порівняти статистичну залежність криптограм і відкритого тексту.

Варіанти завдань наведено у табл. 4.

Таблиця 4

Варіанти завдання

Варіанти	Метод шифрування
1	2
1	Шифр Плейфейера. Поліалфавітна заміна
2	Перестановочний шифр із ключовим словом. Шифр із автоключем з використанням криптограми
3	Шифр простої заміни. Шифр із автоключем з використанням відкритого тексту
4	Афінна криптосистема. Поліалфавітна заміна

Закінчення табл. 4

1	2
5	Шифр Цезаря. Шифр Віженера
6	Шифр Цезаря із ключовим словом. Шифр із автоключем з використанням відкритого тексту
7	Матрична перестановка. Поліалфавітна заміна
8	Шифр Плейфейера. Шифр із автоключем з використанням криптограми
9	Перестановочний шифр із ключовим словом. Поліалфавітна заміна
10	Шифр простої заміни. Шифр Віженера
11	Афінна криптосистема. Шифр із автоключем з використанням відкритого тексту
12	Шифр Цезаря. Шифр із автоключем з використанням криптограми

Завдання 2

Ви є користувачем розподіленої захищеної системи з 6 користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (розшифрування) RSA і виробляти або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувач	Параметр системи n		Ключі користувачів	
	p	q	секретний – d	відкритий – e
A	11	23	19	
B	17	19		137
C	11	17	37	
D	13	19		67
E	17	23	111	
F	13	17		97

Ви користувач "A".

Перевірити, що ваші ключі (відкритий і особливий) відібрані правильно.

Розшифруйте повідомлення M, яке отримано від користувача "F".

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	геш-код	ЦП
Шифрування RSA	F	A	67	--	--

Завдання 3

Виконати аналіз погроз безпеки підприємства, на якому працює студент. Розробити політику безпеки підприємства, в якій зазначити типи конфіденційної інформації, методи криптографічного захисту та методи мережного захисту.

7. Контрольні запитання для самодіагностики

1. Відповідно до "Помаранчевої книги" під безпечною системою розуміється "система, у якій керування доступом до формації здійснюють тільки авторизовані особи або процеси, що діють від їхнього імені, що мають право змінювати яким-небудь способом або видаляти інформацію", чи ні.

2. Які послуги безпеки використовуються для забезпечення захисту від розглянутих загроз відповідно до міжнародних стандартів ISO 7498, ISO/IEC 10181.

3. Секретна система це сукупність криптограм і відкритих текстів, чи ні.

4. Що таке однобічна функція з люком?

5. Що забезпечує протокол обміну повідомлень, у якім використовується відкритий ключ одержувача?

6. Протокол обміну повідомлень, у якому використовується особистий ключ відправника й відкритий ключ одержувача забезпечує конфіденційність і автентичність, чи ні?

7. Повідомлення разом із приєднаним до нього шляхом конкатенації геш-кодом шифрується методами симетричного шифрування, при цьому забезпечується конфіденційність і цифровий підпис, чи ні?

8. Шифрується тільки геш-код засобами шифрування з відкритим ключем з використанням особистого ключа відправника, при цьому забезпечується автентичність і цілісність або цифровий підпис.

9. Шифрується симетричним алгоритмом повідомлення разом з геш-кодом, шифрованим відкритим ключем, при цьому забезпечується конфіденційність і ЦП або конфіденційність і цілісність та цифровий підпис.

10. Чим визначається стійкість геш-коду – довжиною повідомлення або довжиною ключа.

11. У пакет системи PGP включений пакет стиску – ZIP або RAR.

12. Для чого призначений транспортний режим у протоколах AH і ESP.

13. Для чого призначений тунельний режим у протоколах AH і ESP.

14. На чому ґрунтується стійкість цифрового підпису Ель-Гамаля.

15. Яку послугу безпеки забезпечує система Kerberos на основі симетричного шифрування.

16. До спеціальних механізмів безпеки зараховують шифрування, цифровий підпис, конфіденційність, цілісність даних, приналежність;

або шифрування, цифровий підпис, конфіденційність, автентифікація, мітки безпеки, виявлення подій.

8. Індивідуально-консультативна робота

Індивідуально-консультативні заняття (ІКЗ) – вид навчального заняття, при якому студент отримує від викладача відповіді на конкретні запитання або пояснення певних теоретичних положень чи аспектів їх практичного застосування.

Кожна кафедра складає розклад консультацій із зазначенням днів, часу, місця їх проведення та викладачів, які консультують. ІКЗ проводяться, як правило, індивідуально. Вони мають на меті роз’яснення питань, які виникають у тих, хто навчається, при самостійному вивченні навчального матеріалу та виконанні домашніх завдань, поглиблення та закріплення знань з окремих питань та тем дисциплін, надання методичної допомоги у виборі раціональних методів самостійної роботи. При необхідності можуть проводитись і групові ІКЗ.

Відвідання ІКЗ студентами добровільне. Проте, кафедри можуть викликати на співбесіду тих студентів, які у процесі навчання не показують твердих знань і, на думку викладачів, не працюють над дисципліною. Консультуючи студентів, викладач одночасно знайомиться з тим, як вони вивчають рекомендовану літературу, дає поради та вказівки про методи роботи над навчальним матеріалом, які сприяють глибокому та міцному його засвоєнню.

ІКЗ не слід перетворювати у додаткові заняття. На них не рекомендується виконувати за тих, хто навчається, або спільно з ними

домашні завдання. Зі спеціальних та технічних дисциплін не допускається розкриття рішень, які ті, хто навчається, повинні приймати самостійно. Консультації не повинні перетворюватися в форму "підтягування" студентів перед заліками та екзаменами. Вони також не є формою перевірки знань. Знання навчальної дисципліни, які показані студентами у ході ІКЗ, не повинні впливати на екзаменаційну або залікову оцінку.

Індивідуально-консультативна робота здійснюється за графіком індивідуально-консультативної роботи у формі: індивідуальних занять, консультацій, перевірки виконання індивідуальних завдань, перевірки та захисту завдань, що винесені на поточний контроль тощо.

Індивідуально-консультативна робота з теоретичної частини дисципліни проводиться у вигляді:

1) індивідуальних консультацій (запитання – відповідь стосовно проблемних питань теоретичного матеріалу дисципліни);

2) групових консультацій (розгляд типових прикладів, практики впровадження та використання нових методів та методик у виробничу практику).

Індивідуально-консультативна робота з практичної частини дисципліни проводиться у вигляді:

1) індивідуальних консультацій (розгляд практичних завдань стосовно яких виникли запитання);

2) групових консультацій (розгляд практичних ситуацій, рольових ігор, які потребують колективного обговорення).

Індивідуально-консультативна робота для комплексної оцінки засвоєння програмного матеріалу проводиться у вигляді:

1) індивідуального захисту самостійних та індивідуальних завдань;

2) підготовки рефератів для виступу на науковому семінарі,

3) підготовки рефератів для виступу на науковій конференції.

9. Методики активізації процесу навчання

При викладенні навчальної дисципліни для активізації навчального процесу передбачено застосування сучасних навчальних технологій, таких як: проблемні лекції, роботи в малих групах, розігрування ігрових ситуацій, "мозковий штурм". Розподіл форм та методів активізації процесу навчання за темами навчальної дисципліни наведено в табл. 5.

Таблиця 5

Розподіл форм та методів активізації процесу навчання за темами навчальної дисципліни

Тема	Практичне застосування навчальних технологій
Тема 1. Огляд безпеки системи	Проблемна лекція "Визначення базових засад захисту інформації в інформаційної системі підприємства"
Тема 13. Протоколи автентичності Тема 14. Цифрові підписи	Міні-лекція "Класифікація та огляд національних та міжнародних стандартів захисту інформації. Визначення перспективного напряму гармонізації міжнародних стандартів"
Тема 6. Шифрування даних	Кейс "Проведення криптоанализу класичних шифрів". Міні-лекція "Методика визначення криостійкості та дослідження основних характеристик симетричних та асиметричних криптосистем"
Тема 12. Алгоритми з відкритим ключем	Проблемна лекція "Визначення засобів захисту від НСД в інформаційної системі підприємства. Розгортання інфраструктури відкритих ключів". Ділова гра "Обґрунтування вибору механізмів захисту для забезпечення ефективного використання інформації на підприємстві"

Проблемні лекції – спрямовані на розвиток логічного мислення студентів і характеризуються тим, що коло питань теми обмежується двома-трьома ключовими моментами, увага студентів концентрується на матеріалі, що не знайшов відображення в підручниках, використовується досвід закордонних навчальних закладів з роздачею студентам під час лекцій друкованого матеріалу та виділенням головних висновків з питань, що розглядаються. При читанні лекцій студентам даються питання для самостійного розмірковування, проте лектор сам відповідає на них, не чекаючи відповідей студентів. Система питань в ході лекції відіграє активізуючи роль, примушує студентів сконцентруватися і почати активно мислити в пошуках правильної відповіді.

Міні-лекції – передбачають виклад навчального матеріалу за короткий проміжок часу й характеризуються значною ємністю, складністю логічних побудов, образів, доказів та узагальнень. Міні-лекції проводяться, як правило, як частина заняття-дослідження.

Робота в малих групах – використовується з метою активізації роботи студентів при проведенні семінарських і практичних занять. Це так звані групи психологічного комфорту, де кожен учасник відіграє свою особливу роль і певними своїми якостями доповнює інших. Використання цієї технології дає змогу структурувати практично-семінарські заняття за формою і змістом, створює можливості для участі кожного студента в роботі за темою заняття, забезпечує формування особистісних якостей та досвіду соціального спілкування.

Кейс-метод (метод аналізу конкретних ситуацій) – дає змогу наблизити процес навчання до реальної практичної діяльності спеціалістів і передбачає розгляд виробничих, управлінських та інших ситуацій, складних конфліктних випадків, проблемних ситуацій, інцидентів у процесі вивчення навчального матеріалу.

Презентації – виступи перед аудиторією – використовуються для представлення певних досягнень, результатів роботи групи, звіту про виконання індивідуальних завдань, інструктажу, демонстрації нових товарів і послуг.

Рольові ігри (інсценізації) – форма активізації студентів, за якої вони задіяні в процесі інсценізації певної виробничої ситуації у ролі безпосередніх учасників подій.

Модерація – це метод, який допомагає групам розглядати теми, проблеми, задачі зосереджуючись на змісті цілеспрямовано і ефективно при самостійній участі кожного у вільній колегіальній атмосфері. Модерація як спосіб проведення обговорення, швидко призводить до конкретних результатів, дає можливість всім присутнім брати участь в процесі вироблення рішень, відчуваючи при цьому свою повну відповідальність за результат.

10. Система поточного та підсумкового контролю знань студентів

У процесі навчання студенти отримують необхідні знання під час лекційних занять, виконуючи лабораторні роботи щодо захисту інформації в інформаційних системах підприємств.

Оцінювання знань, вмінь та навичок студентів враховує види занять, які згідно з програмою навчальної дисципліни "Технології захисту інформації" передбачають лекційні та лабораторні заняття, а також самостійну роботу та виконання індивідуальних завдань.

Перевірка та оцінювання знань студентів може проводитись кількома методами:

Оцінювання знань студента під час лабораторних занять.

Оцінювання виконання індивідуального завдання.

Виконання завдань для самостійної роботи.

Проведення проміжного контролю.

Проведення поточно-модульного контролю.

Проведення підсумкового контролю.

Порядок поточного оцінювання знань студентів

Поточне оцінювання здійснюється під час проведення лабораторних занять і має мету – перевірку рівня підготовленості студента до виконання конкретної роботи. Об'єктами поточного контролю є:

1) активність та результативність роботи студента протягом семестру над вивченням програмного матеріалу дисципліни; відвідування занять;

2) виконання проміжного контролю;

3) виконання модульного контрольного завдання.

Контроль систематичного виконання самостійної роботи та активності на лабораторних заняттях

Оцінювання проводиться за 12-ти бальною шкалою за такими критеріями:

розуміння, ступінь засвоєння теорії та методології проблем, що розглядаються;

ступінь засвоєння фактичного матеріалу навчальної дисципліни;

ознайомлення з рекомендованою літературою, а також із сучасною літературою з питань, що розглядаються;

вміння поєднувати теорію з практикою при розгляді задачі оброблення облікової інформації, розробленні постановки задачі, алгоритму та технології її вирішення, технологічного забезпечення при виконанні індивідуальних завдань та завдань, винесених на розгляд в аудиторії;

логіка, структура, стиль викладу матеріалу в письмових роботах і при виступах в аудиторії, вміння обґрунтовувати свою позицію, здійснювати узагальнення інформації та робити висновки.

Оцінка "відмінно" (10 – 12 балів) ставиться за умови відповідності індивідуального завдання студента, або його усної відповіді усім п’ятьом зазначеним критеріям. Відсутність тієї або іншої складової знижує оцінку на відповідну кількість балів.

При оцінюванні індивідуальних завдань увага також приділяється якості, самостійності та своєчасності здачі виконаних завдань викладачу (згідно з графіком навчального процесу).

Оцінювання знань студента під час виконання завдань для самостійної роботи проводиться за 12-ти бальною шкалою**.**

Модульний контроль

Проміжний модульний контроль рівня знань передбачає виявлення опанування студентом матеріалу лекційного модуля та вміння застосовувати його для вирішення практичної ситуації і проводиться у вигляді тестування. При цьому тестове завдання може містити як запитання, що стосуються суто теоретичного матеріалу, так і запитання, спрямовані на вирішення невеличкого практичного завдання.

Тестове завдання містить запитання одиничного і множинного вибору різного рівня складності.

Для оцінювання рівня відповідей студентів на тестові завдання використовуються такі критерії оцінювання:

Кількість балів	Оцінка
91,64 – 100	12
83,31 – 91,63	11
74,98 – 83,3	10
66,65 – 74,97	9
58,32 – 66,64	8
49,99 – 58,31	7
41,66 – 49,98	6
33,33 – 41,65	5
25 – 33,32	4
16,67 – 24,99	3
8,34 – 16,66	2
0 – 8,33	1

Метою вирішення тестових завдань з навчальної дисципліни є засвоєння студентами теоретичних знань з методів та процедур

забезпечення захист інформації в ІС, придбання практичних вмінь та навичок в розробленні постановки задачі, її алгоритму та технологічного забезпечення.

Відповідно до Галузевого стандарту освіти тестові завдання спрямовані на забезпечення виконання студентами виробничих функцій (технічних, виконавських, проектувальних, організаційних), задач діяльності (професійних, соціально-виробничих і соціально-побутових) та класів задач діяльності (стереотипних, діагностичних і евристичних), згідно яких має здійснюватися підготовка фахівця певного рівня кваліфікації.

Проведення підсумкового контролю. Умовою допуску підсумкового контролю є позитивні оцінки з змістового контролю знань. Підсумковий контроль знань студентів здійснюється у формі проведення іспиту за 12-ти бальною шкалою.

Питання іспиту включають такі завдання:

теоретичне запитання;

практичні завдання різного ступеня складності.

Зміст практичних завдань екзаменаційних білетів побудований таким чином, щоб перевірити ступінь відповідності підготовки студента до вимог положень освітньо-кваліфікаційної характеристики за напрямом підготовки. У першу чергу перевіряється здатність студента самостійно оцінювати рівень безпеки в інформаційної системі, визначати які механізми і протоколи потрібні для забезпечення послуг конфіден-ційності, автентичності та цілісності інформаційного обміну, здійснювати аналіз та синтез криптографічних механізмів, які використовуються в інформаційних системах, а також графічно обґрунтовувати використання можливих схем застосування програмних та програмно-апаратних засобів забезпечення безпеки в інформаційної системі.

Кожне з практичних завдань та теоретичне питання оцінюється за 12-бальною системою з подальшою підсумковою оцінкою за виконання всього екзаменаційного завдання.

Передбачається використовувати такі критерії для виставлення оцінок:

Завдання 1 (*теоретичне*)

Оцінка 12 балів. Відповідь на теоретичне запитання дана повно та відповідає відповідним стандартам. Кожному з показників наведено відповідне пояснення, Наведені приклади їх застосування у відповідних

міжнародних стандартах та протоколах, визначені рівні еталонної моделі взаємодії відкритих систем, на яких виконуються відповідні показники або механізми, вказані задачі, які розв'язують показники або механізми, їх переваги і недоліки.

Оцінка 11 балів. Відповідь на теоретичне запитання дана повно та відповідає відповідним стандартам. Кожному з показників наведе відповідне пояснення, наведені приклади їх застосування у відповідних міжнародних стандартах та протоколах, визначені рівні еталонної моделі взаємодії відкритих систем, на яких виконуються відповідні показники або механізми, вказані задачі, які розв'язують показники або механізми, але не вказані їх переваги і недоліки.

Оцінка 10 балів. Відповідь на теоретичне запитання дана повно та відповідає відповідним стандартам. Кожному з показників наведено відповідне пояснення, Наведені приклади їх застосування в відповідних міжнародних стандартах та протоколах, визначені рівні еталонної моделі взаємодії відкритих систем, на яких виконуються відповідні показники або механізми, але не вказані задачі, які розв'язують показники (механізми).

Оцінка 9 балів. Відповідь на теоретичне запитання дана повно та відповідає відповідним стандартам. Кожному з показників наведено відповідне пояснення, Наведені приклади їх застосування у відповідних міжнародних стандартах та протоколах, але не визначені рівні еталонної моделі взаємодії відкритих систем, на яких виконуються відповідні показники або механізми, не вказані задачі, які розв'язують показники або механізми.

Оцінка 8 балів. Відповідь на теоретичне запитання дана неповно та відповідає відповідним стандартам. Для 2/3 показників наведено відповідне пояснення, наведені приклади їх застосування в відповідних міжнародних стандартах та протоколах, але не визначені рівні еталонної моделі взаємодії відкритих систем, на яких виконуються відповідні показники або механізми, не вказані задачі, які розв'язують показники (механізми).

Оцінка 7 балів. Відповідь на теоретичне запитання дана неповно та відповідає відповідним стандартам. Для 1/2 показників наведено відповідне пояснення, наведені приклади їх застосування в відповідних міжнародних стандартах та протоколах, але не визначені рівні еталонної моделі взаємодії відкритих систем, на яких виконуються відповідні показники або механізми, не вказані задачі, які розв'язують показники (механізми).

Оцінка 6 балів. Відповідь на теоретичне запитання дана неповно та не в повному обсязі відповідає відповідним стандартам. Для 1/2 показників наведено відповідне пояснення, але не наведені приклади їх застосування у відповідних міжнародних стандартах та протоколах, не визначені рівні еталонної моделі взаємодії відкритих систем, на яких виконуються відповідні показники або механізми, не вказані задачі, які розв'язують показники (механізми).

Оцінка 5 балів. Відповідь на теоретичне запитання дана неповно та не в повному обсязі відповідає відповідним стандартам. Для менш ніж 1/2 показників наведено відповідне пояснення, але не наведені приклади їх застосування у відповідних міжнародних стандартах та протоколах, не визначені рівні еталонної моделі взаємодії відкритих систем, на яких виконуються відповідні показники або механізми, не вказані задачі, які розв'язують показники (механізми).

Оцінка 4 бали. Відповідь на теоретичне запитання дана неповно та не в повному обсязі відповідає відповідним стандартам. Відповідні показники (механізми) лише перераховані, але не наведено відповідне пояснення для кожного показника, не наведені приклади їх застосування у відповідних міжнародних стандартах та протоколах, не визначені рівні еталонної моделі взаємодії відкритих систем, на яких виконуються відповідні показники або механізми, не вказані задачі, які розв'язують показники (механізми).

Оцінка 3 бали. Відповідь на теоретичне запитання не дана. Показники (механізми) лише перераховані на 2/3, але не наведено відповідне пояснення для кожного показника, не Наведені приклади їх застосування в відповідних міжнародних стандартах та протоколах, не визначені рівні еталонної моделі взаємодії відкритих систем, на яких виконуються відповідні показники або механізми, не вказані задачі, які розв'язують показники (механізми).

Оцінка 2 бали. Відповідь на теоретичне запитання не дана. Відповідні показники (механізми) лише перераховані на 1/2 і не відповідають відповідним стандартам, не наведено відповідне пояснення для кожного показника, не наведені приклади їх застосування у відповідних міжнародних стандартах та протоколах, не визначені рівні еталонної моделі взаємодії відкритих систем, на яких виконуються відповідні показники або механізми, не вказані задачі, які розв'язують показники (механізми).

Оцінка 1 бал. Відповідь на теоретичне запитання відсутня.

Завдання 2 (*практичне*)

Оцінка 12 балів. Практичне завдання виконано бездоганно з повним обґрунтуванням кожного етапу виконання завдання, зроблені повні висновки та узагальнення. Наведені алгоритми шифрування/розшифрування з поясненнями, сформована криптограма відповідає алгоритму шифрування, стійкість алгоритму шифрування оцінено частотним криптоаналізом.

Оцінка 11 балів. Практичне завдання виконано повністю з досить повним обґрунтуванням кожного етапу виконання завдання, зроблені досить повні висновки та узагальнення. Наведені алгоритми шифрування/розшифрування з поясненнями, сформована криптограма відповідає алгоритму шифрування, стійкість алгоритму шифрування оцінено частотним криптоаналізом.

Оцінка 10 балів. Практичне завдання виконано повністю з достатнім обґрунтуванням кожного етапу виконання завдання, зроблені достатні висновки та узагальнення. Наведені алгоритми шифрування/розшифрування з поясненнями, сформована криптограма відповідає алгоритму шифрування, але стійкість алгоритм шифрування неоціненно частотним криптоаналізом.

Оцінка 9 балів. Практичне завдання виконано повністю з достатнім обґрунтуванням кожного етапу виконання завдання, зроблені достатні висновки та узагальнення. Наведені алгоритми шифрування/розшифрування, сформована криптограма відповідає алгоритму шифрування.

Оцінка 8 балів. Практичне завдання виконано повністю. Наведені алгоритми шифрування/розшифрування, сформована криптограма відповідає алгоритму шифрування.

Оцінка 7 балів. Практичне завдання виконано повністю. Наведений тільки алгоритм шифрування, сформована криптограма відповідає алгоритму шифрування.

Оцінка 6 балів. Практичне завдання виконано повністю. Сформована криптограма відповідає алгоритму шифрування, але не наведені алгоритми шифрування/розшифрування.

Оцінка 5 балів. Практичне завдання виконано неповністю. Сформована криптограма відповідає алгоритму шифрування, але окремі символи зашифровані неправильно.

Оцінка 4 бали. Практичне завдання виконано неповністю. Сформована криптограма відповідає алгоритму шифрування, але 1/2 символів зашифровані неправильно.

Оцінка 3 бали. Практичне завдання не виконано. Сформована криптограма не відповідає алгоритму шифрування, або більш 1/2 символів зашифровані неправильно.

Оцінка 2 бали. Практичне завдання не виконано. Сформована криптограма не відповідає алгоритму шифрування, або більш 2/3 символів зашифровані неправильно.

Оцінка 1 бал. Відповідь на практичне запитання відсутня.

Завдання 3, 5 (*практичні*)

Оцінка 12 балів. Практичне завдання виконано бездоганно з повним обґрунтуванням кожного етапу виконання завдання, зроблені повні висновки та узагальнення. Наведений протокол обміну відповідає вимогам відповідного стандарту, наведені алгоритми шифрування/розшифрування з повними поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), визначені переваги і недоліки обґрунтовані. Наведені механізми та послуги, в яких використовуються відповідні протоколи (схеми шифрування).

Оцінка 11 балів. Практичне завдання виконано бездоганно з повним обґрунтуванням кожного етапу виконання завдання, зроблені повні висновки та узагальнення. Наведений протокол обміну відповідає вимогам відповідного стандарту, наведені алгоритми шифрування/розшифрування з повними поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), визначені переваги і недоліки обґрунтовані, але не наведені механізми та послуги, в яких використовуються відповідні протоколи (схеми шифрування).

Оцінка 10 балів. Практичне завдання виконано повністю з досить повним обґрунтуванням кожного етапу виконання завдання, зроблені повні висновки та узагальнення. Наведений протокол обміну відповідає вимогам відповідного стандарту, наведені алгоритми шифрування/розшифрування з повними поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), визначені основні переваги і недоліки обґрунтовані.

Оцінка 9 балів. Практичне завдання виконано повністю з обґрунтуванням кожного етапу виконання завдання. Наведений протокол обміну відповідає вимогам відповідного стандарту, наведені алгоритми шифрування/розшифрування з повними поясненнями, сформована криптограма

(повідомлення) відповідає алгоритму шифрування (розшифрування), визначені основні переваги і недоліки обґрунтовані.

Оцінка 8 балів. Практичне завдання виконано повністю з обґрунтуванням кожного етапу виконання завдання. Наведений протокол обміну відповідає вимогам відповідного стандарту, наведені алгоритми шифрування/розшифрування з повними поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), визначені основні переваги і недоліки.

Оцінка 7 балів. Практичне завдання виконано повністю. Наведений протокол обміну відповідає вимогам відповідного стандарту, наведені алгоритми шифрування/розшифрування з поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), визначені основні переваги.

Оцінка 6 балів. Практичне завдання виконано повністю. Наведений протокол обміну відповідає вимогам відповідного стандарту, наведені алгоритми шифрування/розшифрування, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування).

Оцінка 5 балів. Практичне завдання виконано неповністю. Наведений протокол обміну відповідає вимогам відповідного стандарту, наведені алгоритми шифрування/розшифрування, але сформована криптограма або повідомлення не відповідають алгоритму шифрування або розшифрування.

Оцінка 4 бали. Практичне завдання виконано неповністю. Наведений протокол обміну відповідає вимогам відповідного стандарту, наведені алгоритми шифрування/розшифрування, але сформована криптограма і повідомлення не відповідають алгоритму шифрування/розшифрування.

Оцінка 3 бали. Практичне завдання не виконано. Наведений протокол обміну не відповідає вимогам відповідного стандарту, не наведені алгоритми шифрування/розшифрування, сформована криптограма і повідомлення не відповідають алгоритму шифрування/розшифрування.

Оцінка 2 бали. Практичне завдання не виконано. Протокол обміну не наведений, не наведені алгоритми шифрування/розшифрування, сформована криптограма і повідомлення не відповідають алгоритму шифрування/розшифрування.

Оцінка 1 бал. Відповідь на практичне запитання відсутня.

Завдання 4 (*практичне*)

Оцінка 12 балів. Практичне завдання виконано бездоганно з повним обґрунтуванням кожного етапу виконання завдання, зроблені повні висновки та узагальнення. Наведені схеми локальних обчислювальних мереж (ЛОМ) відповідають відповідним токологіям і характеристикам ЛОМ, обґрунтовані та запропоновані необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами корпоративної обчислювальної мережі (КОМ). Визначені переваги і недоліки використаних програмно-апаратних засобів захисту. Наведені пропозиції щодо покращення рівня безпеки КОМ.

Оцінка 11 балів. Практичне завдання виконано повністю з досить повним обґрунтуванням кожного етапу виконання завдання, зроблені повні висновки та узагальнення. Наведені схеми ЛОМ відповідають відповідним токологіям і вимогам ЛОМ, обґрунтовані та запропоновані необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами КОМ. Визначені переваги і недоліки використаних програмно-апаратних засобів захисту.

Оцінка 10 балів. Практичне завдання виконано повністю з досить повним обґрунтуванням кожного етапу виконання завдання, зроблені повні висновки та узагальнення. Наведені схеми ЛОМ відповідають відповідним токологіям і вимогам ЛОМ, обґрунтовані та запропоновані необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами КОМ. Визначені основні переваги використаних програмно-апаратних засобів захисту.

Оцінка 9 балів. Практичне завдання виконано повністю з обґрунтуванням окремих етапів виконання завдання. Наведені схеми ЛОМ відповідають відповідним токологіям і вимогам ЛОМ, обґрунтовані та запропоновані необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами КОМ.

Оцінка 8 балів. Практичне завдання виконано повністю. Наведені схеми ЛОМ в основному відповідають відповідним токологіям і вимогам ЛОМ, запропоновані необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами корпоративної обчислювальної мережі (КОМ). Наведені окремі переваги і недоліки засобів захисту.

Оцінка 7 балів. Практичне завдання виконано повністю. Наведені схеми ЛОМ в основному відповідають відповідним токологіям, але підключення ПК не відповідає вимогам ЛОМ, запропоновані необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами КОМ.

Оцінка 6 балів. Практичне завдання виконано повністю. Наведені схеми ЛОМ відповідають відповідним токологіям, але підключення ПК і програмно-апаратних засобів захисту не відповідає вимогам ЛОМ, запропоновані необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами КОМ.

Оцінка 5 балів. Практичне завдання виконано повністю. Наведені схеми ЛОМ не відповідають відповідним токологіям, також підключення ПК і програмно-апаратних засобів захисту не відповідає вимогам ЛОМ, запропоновані окремі протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами КОМ.

Оцінка 4 бали. Практичне завдання виконано повністю. Наведені схеми ЛОМ не відповідають відповідним токологіям, відсутні підключення ПК; підключення програмно-апаратних засобів захисту не відповідає вимогам ЛОМ, запропоновані окремі протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами КОМ.

Оцінка 3 бали. Практичне завдання не виконано. Наведені схеми ЛОМ не відповідають відповідним токологіям, відсутні підключення ПК і програмно-апаратних засобів захисту, запропоновані окремі протоколи і програмно-апаратні засоби не мають логіки їх застосування при забезпеченні конфіденційного обміну інформацією між користувачами КОМ.

Оцінка 2 бали. Практичне завдання не виконано. Наведені схеми ЛОМ не відповідають відповідним токологіям, відсутні підключення ПК і програмно-апаратних засобів захисту, запропоновані протоколи і програмно-апаратні засоби не мають логіки їх застосування при забезпеченні конфіденційного обміну інформацією між користувачами КОМ.

Оцінка 1 бал. Відповідь на практичне запитання відсутня.

Приклад запитань іспиту

Завдання 1 (*теоретичне*)

Назвіть основні послуги та механізми безпеки відповідно до стандартів ISO 7498, ISO\IES 10181.

Завдання 2 (*практичне*)

Зашифруйте і розшифрувати за допомогою поліалфавітного методу шифрування відкритий текст. *Відкритий текст:* конфіденційність. *Ключ(і):* К(2-3-4-1).

Алфавіт(и):

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$А_{откр}$	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
$А_{шифр1}$	й	ц	у	к	е	н	г	ш	щ	з	х	ъ	ф	ы	в	а	п	р	о	л	д	ж	э	я	ч	с	м	и	т	ь	б	ю
$А_{шифр2}$	я	ю	э	ь	ы	ъ	щ	ш	ч	ц	х	ф	у	т	с	р	п	о	н	м	л	к	й	и	з	ж	е	д	г	в	б	а
$А_{шифр3}$	п	р	г	ш	к	е	й	ц	у	ъ	ф	о	л	д	ж	щ	з	х	ч	с	н	б	ю	и	э	я	т	ь	ы	в	а	м
$А_{шифр4}$	ь	к	е	д	ж	э	а	м	ъ	у	щ	з	х	ф	о	л	б	п	р	г	ш	ю	й	ц	и	ч	с	н	я	т	ы	в

Завдання 3 (*практичне*)

Побудуйте протокол обміну інформації між користувачами А і В за допомогою алгоритму хешування для забезпечення конфіденційності. Визначити переваги та недоліки даного протоколу. Порівняйте з протоколами асиметричного шифрування.

Завдання 4 (*практичне*)

У корпоративній мережі компанії, що розташовується в 2-х будинках (4 поверхи та 2 поверхи відповідно), розміщені рівномірно 12 ПК (у першому – 8 комп’ютерів, у другому – 4), які об’єднані в автономні локальні мережі за технологіями Token Ring і Ethernet відповідно. Розробити структурну схему захисту корпоративної мереж компанії, обґрунтувати та запропонувати необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами другого будинку; забезпечити надійний захист при виході користувачів до мережі Інтернет за допомогою NAT другої форми, proxy-сервера та шлюзу прикладного рівня з брандмауером.

Завдання 5 (*практичне*)

Ви є користувачем розподіленої захищеної системи з 6 користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (расшифрування) RSA і виробляти або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувач	Параметр системи n		Ключі користувачів	
	p	q	секретний – d	відкритий – e
A	11	23	19	
B	17	19		137
C	11	17	37	
D	13	19		67
E	17	23	111	
F	13	17		97

Ви користувач "A".

Перевірити, що ваші ключі (відкритий і особливий) відібрані правильно.

Расшифруйте повідомлення M, яке отримано від користувача "F".

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	геш-код	ЦП
Шифрування RSA	F	A	67	–	–

Загальна оцінка за виконання всіх екзаменаційних завдань розраховується за формулою:

$$О_{екз} = \lfloor (Z1 + Z2 + Z3 + Z4 + Z5) / 5 \rfloor,$$

де Z1, Z2, Z3, Z4, Z5 – оцінка за виконане завдання екзаменаційного білету.

Загальна модульна оцінка складається з поточної оцінки, яку студент отримує під час лабораторних занять, оцінки за виконання індивідуального завдання та оцінки за виконання модульної контрольної роботи.

Підсумкова оцінка з навчальної дисципліни розраховується за формулою:

$$О_{підсумкова} = (ТМ1 + ТМ2 + ПМ1 + ПМ2) / 4 * 0{,}4 + О_{екз} * 0{,}6$$

де ТМ1 – оцінка за теоретичний модуль 1;

ТМ2 – оцінка за теоретичний модуль 2;

ПМ1 – оцінка за практичний модуль 1;

ПМ 2 – оцінка за практичний модуль 2;

$О_{екз}$ – оцінка за екзамен.

Підсумкова оцінка з дисципліни згідно з Методикою переведення показників успішності знань студентів Університету в систему оцінювання за шкалою ECTS конвертується в підсумкову оцінку за шкалою ECTS (табл. 6).

Таблиця 6

Переведення показників успішності знань студентів ХНЕУ в систему оцінювання за шкалою ECTS

Відсоток студентів, які успішно досягають відповідної оцінки	Оцінка за шкалою ECTS		Оцінка за бальною шкалою ХНЕУ	Оцінка за національною шкалою
10	відмінне виконання	A	12 – 11	відмінно
25	вище середнього рівня	B	10	
30	взагалі робота правильна, але з визначеною кількістю помилок	C	9 – 7	добре
25	непогано, але зі значною кількістю недоліків	D	6	задовільно
10	виконання задовольняє мінімальні критерії	E	5 – 4	
–	потрібне повторне перескладання	FX	3	незадовільно
–	повторне вивчання дисципліни	F	2 – 1	

11. Рекомендована література

11.1. Основна

1. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи / О. А. Баранов. – К. : Видавничий дім "СофтПрес", 2005. – 316 с.

2. Венбо М. Современная криптография: теория и практика : пер. с англ. / М.Венбо – М. : Издательский дом "Вильямс", 2005. – 768 с.

3. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. – Львів : ВНТЛ, 1998. – 248 с.

4. Горбатов В. С. Основы технологии PKI / В. С.Горбатов, О. Ю. Полянская – М. : Горячая линия – Телеком, 2004. – 248 с.

5. Гребенчук В. Г. Цифровая стеганография / В. Г. Гребенчук, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.

6. Грибунин В. Г. Цифровая стеганографія / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Прес, 2002. – 272 с.

7. Зима В. М. Безопасность глобальніх сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. – 2-е изд. – СПб. : БХВ-Петербург, 2003. – 368 с.

8. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.

9. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 510 с.

10. Ленков С. В. Методы и средства защиты информации. В 2-х томах / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. Т.II. Информационная безопасность. – К. : Арий, 2008. – 344 с.

11. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров – М. : ДМК, 2000. – 448 с.

12. Поповский В. В. Защита информации в телекоммуникационных системах : учебник : в 2 т. / В. В. Поповский, А. В. Персиков. – Х. : ООО "Компания СМИТ", 2006. – Т. 1. – 292 с.

13. Поповский В. В. Защита информации в телекоммуникационных системах : учебник : в 2 т. / В. В. Поповский, А. В. Персиков. – Х. : ООО "Компания СМИТ", 2006. – Т. 2. – 252 с.

14. Столлингс В. Криптография и защита сетей: принципы и практика. – 2-е изд. / В. Столлингс; пер. с англ. – М. : Издательский дом "Вильямс", 2001. – 672 с.

15. Хайнс Б. Руководство по безопасности Windows Server 2008 / Б. Хайнс, Б. Курри, Д. Стин, Р. Харриссон. – Microsoft, 2008. – 326 с.

16. Хорошко В. А. Методы и средства зашиты информации / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с.

17. Чмора А. Л. Современная прикладная криптография / А. Л. Чмора. – М. : Гелиос АРВ, 2001. – 256 с.

18. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и Техника, 2004. – 384 с.

11.2. Ресурси мережі Інтернет

19. http://bezopasnost.biz.

20. http://dstszi.gov.ua.

21. Журнал "Информационные технологии. Аналитические материалы" [Электронный ресурс]. – Режим доступа : http://it.ridne.net.

22. Історія розвитку інформаційних технологій в Україні [Електронний ресурс]. – Режим доступу : http://www.icfcst.kiev.ua/MUSEUM/IT_u.html.

23. Нормативные акты Украины [Электронный ресурс]. – Режим доступа : www.nau.kiev.ua.

24. Центр информационных технологий [Электронный ресурс]. – Режим доступа : http://www.citmgu.ru.

25. Information Technology Security Evaluation Criteria, v. 1.2. – Office for Official publications of the European Communities, 1991 [Electronic resource]. – Access mode : www.fbi.gov.

26. www.pgpi.org.

27. linuxpage.ru.

28. www.securityfocus.com.

29. www.sysinternals.com.

30. www.zdnet.ru.

31. www.submarine.ru.

32. www.securitylab.ru.

33. http://www.osp.ru.

34. http://zakon1.rada.gov.ua.

35. http://www.cyberguru.ru.

Зміст

НАВЧАЛЬНЕ ВИДАННЯ

Робоча програма
навчальної дисципліни
"ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ"

для студентів напряму підготовки
6.050101 "Комп'ютерні науки"
всіх форм навчання

Укладачі: **Кузнецов** Олександр Олександрович
Євсеєв Сергій Петрович
Поляков Андрій Олександрович та ін.

Відповідальний за випуск **Пономаренко В. С.**

Редактор **Бутенко В. О.**

Коректор **Бриль В. О.**

План 2012 р. Поз. № 276.
Підп. до друку Формат 60×90 1/16. Папір MultiCopy. Друк Riso.
Ум.-друк. арк. 3,25. Обл.-вид. арк. 4,06. Тираж прим. Зам. №

Видавець і виготівник – видавництво ХНЕУ, 61001, м. Харків, пр. Леніна, 9а

Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи
Дк № 481 від 13.06.2001 р.