МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Робоча програма

навчальної дисципліни

"ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ"

для студентів напряму підготовки "Комп'ютерні науки"

денної форми навчання

Харків. Вид. ХНЕУ, 2008

Затверджено на засіданні кафедри інформаційних систем.
Протокол №5 від 11.12.2007 р.

Р78 Робоча програма навчальної дисципліни "Захист інформації в інформаційних системах" для студентів напряму підготовки "Комп'ютерні науки" денної форми навчання / Укл. С. П. Євсеєв, В. В. Огурцов, А. О. Поляков. – Харків: Вид. ХНЕУ, 2008. – 48 с. (Укр. мов.)

Розкрито принципи побудови систем захисту інформації, застосування механізмів захисту інформації, що засновані на використанні алгоритмів традиційної (симетричної) криптографії, криптографії з відкритим ключем, MAC-кодів і геш-функцій для забезпечення автентичності, цілісності та конфіденційності інформації в інформаційних системах (ІС). Розглянуто основи стеганографічного захисту інформації та особливості побудови інфраструктури відкритих ключів (ІВК).
Рекомендовано для студентів напряму підготовки "Комп'ютерні науки" денної форми навчання.

Вступ

Навчальну дисципліну "Захист інформації в інформаційних системах" віднесено до групи професійно-практичних дисциплін підготовки бакалаврів зі спеціальностей "Інформаційні управляючи системи та технології" та "Комп'ютерний екологи-економічний моніторинг". Вона є невід'ємною частиною циклу професійно-орієнтованої підготовки, необхідної працівникам підприємств незалежно від форми власності та організаційно-правової форми господарювання.

Вивчення дисципліни "Захист інформації в інформаційних системах" дозволяє студентам оволодіти знаннями та вміннями, які створять теоретичний і практичний фундамент, необхідний для аналізу загроз виникаючих при зберіганні, обробленні та передачі інформації; побудові системи захисту інформації на основі використання методів традиційної криптографії та криптографії з відкритим ключем. Ця дисципліна вивчається на четвертому курсі у восьмому семестрі.

Метою навчальної дисципліни є навчання студентів принципам побудови ситем захисту інформації на основі використання алгоритмів симетричної та несиметричної криптографії, MAC-кодів та хеш-функцій щодо забезпечення аутентичності, цілісності та конфіденціальності інформації в ІС.

Предмет навчальної дисципліни – вивчення математичних основ криптографічних перетворень для забезпечення автентичності, цілісності та конфіденціальності інформації на різних рівнях еталонної моделі взаємодії відкритих систем, призначення та принципи дії основних механізмів і протоколів забезпечення захисту інформації, їх взаємозв'язок.

Теоретичними та науковими основами дисципліни є алгебра полів Галуа, теорії захисту інформації та алгебраїчної теорії кодів, теорія цифрових автоматів й теорія складності.

Методичною основою дисципліни є методи і алгоритми алгебраїчної теорії кодів, які базуються на математичному апараті теорії алгебраїчних блокових кодів, теорії імовірності та математичної статистики.

Спосіб досягнення зазначеної мети міститься у використанні в навчально-виховному процесі системи педагогічних заходів і дій, що засновані на реалізації під час занять загальнодидактичних принципів інформаційно-рецептивного, репродуктивного та проблемного методів навчання.

Структура робочої програми навчальної дисципліни "Захист інформації в інформаційних системах" наведена в табл. 1.

Таблиця 1

Структура навчальної дисципліни

<table>
<tr><th>Навчальна дисципліна
підготовка бакалаврів</th><th>Галузь знань, спеціалізація,
освітньо-кваліфікаційний рівень</th><th>Характеристика навчальної
дисципліни</th></tr>
<tr><td>Кількість кредитів відповідних ECTS: 3 кредити,
у тому числі:
змістовних модулів – 1,
самостійна робота; індивідуальне навчально-дослідне завдання (ІНДЗ);
завдання для самостійної роботи</td><td>Шифр і назва галузі знань:
0501 "Інформатика та комп’ютерна техніка".
Шифр та назва напрямку підготовки
6.050101 "Комп’ютерні науки"</td><td>Обов’язкова.
Рік підготовки: 4.
Семестр: 8</td></tr>
<tr><td>Кількість годин:
усього – 108</td><td>Назви спеціалізацій:
"Інформаційні управляючі системи та технології",
"Комп’ютерний еколого-економічний моніторинг"</td><td>Лекції (теоретична підготовка): 10 годин.
Лабораторні роботи: 30 годин.
Самостійна робота: 58 годин.
ІНДЗ: 10 годин</td></tr>
<tr><td>Кількість тижнів викладання – 10.
Кількість годин
за тиждень – 4</td><td>Освітньо-кваліфікаційний рівень бакалавр</td><td>Вид контролю:
Іспит</td></tr>
</table>

Основними завданнями в процесі вивчення дисципліни є: одержання знань з основоположних принципів побудови механізмів захисту інформації на основі алгоритмів симетричної та несиметричної криптографії; одержання знань про основні криптографічні процедури для забезпечення аутентичності, цілісності та конфіденційності інформації; підготовка студента до подальшого поглибленого вивчення спеціальних дисциплін; вироблення навичок самостійного вивчення різноманітних алгоритмів шифрування даних і проведення їх порівняльного аналізу при створенні ефективної системи захисту інформації.

Засобами досягнення мети та вирішення завдань дисципліни є:

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

Навчальна дисципліна базується на знаннях та вміннях, отриманих при вивченні дисциплін "Дискретна математика", "Основи програмування", "Комп'ютерна схемотехніка" та забезпечує підготовку студента за фахом і вивчення наступних спеціальних дисциплін.

Необхідним елементом успішного засвоєння навчального матеріалу дисципліни є самостійна робота студентів з літературою з питань вивчення методів та алгоритмів криптографічного перетворення інформації механізмів і 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 до самопідготовки з переліком питань, що вивчаються самостійно, та конкретних цілей, досягненню яких служить їх обробка. При цьому цілі повинні бути щільно зв'язані з практичними завданнями підготовки студента, як фахівця.

У процесі навчання студенти отримують необхідні знання під час проведення аудиторних занять: лекційних і лабораторних. Також велике значення в процесі вивчення та закріплення знань має самостійна робота студентів. Усі ці види занять розроблені відповідно до положень Болонської декларації.

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

Навчальна дисципліна "Захист інформації в інформаційних системах" є обов'язковою для підготовки бакалаврів комп'ютерних спеціальностей.

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 курсів – схемотехніки. У свою чергу, знання з даної дисципліни забезпечують успішне виконання курсових і дипломних проектів.

У результаті вивчення запропонованої навчальної дисципліни студенти повинні знати:

1. Основні положення законодавства в галузі захисту інформації.
2. Основні терміни та визначення, принципи побудови профілю захисту.
3. Основні міжнародні та національні стандарти з захисту інформації.
4. Основні принципи організації захисту інформації в інформаційних системах.
5. Механізми та протоколи забезпечення конфіденціальності інформації.
6. Механізми й протоколи забезпечення аутентичності інформації в інформаційних системах.
7. Механізми та протоколи цілісності даних в інформаційних системах.
8. Основні види атак, принципи криптоаналізу.
9. Основні напрямки розвитку сучасної криптографії.
10. Механізми та протоколи керування ключами в ІВК інформаційної системи.

Практичні навички, якими оволодівають студенти при вивченні дисципліни:

1. Визначати вимоги та формувати профіль захисту в інформаційних системах.
2. Ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів і протоколів захисту інформації в інформаційних системах.
3. Визначати механізми та протоколи для забезпечення аутентичності інформації.
4. Визначати криптографічні системи для забезпечення конфіденціальності даних в інформаційних системах.
5. Вибирати механізми та протоколи для забезпечення цілісності даних, проводити розрахунки їх потрібних показників.
6. Забезпечувати грамотний підбір програмно-апаратних і програмних засобів для забезпечення необхідного рівня захисту інформації.

7. 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 в цілому.

8. Оформлювати прийняті технічні рішення щодо забезпечення захисту інформації у вигляді комплекту технічної документації, враховуючи необхідний рівень безпеки даних в інформаційної системі фактори можливих атак, а також необхідну кількість механізмів і протоколів захисту під час розробки системи безпеки інформаційних систем.

9. Проводити об'єктивний аналіз ефективності прийнятих технічних рішень щодо забезпечення захисту інформації в інформаційних системах, користуватися математичним та статистичним апаратом щодо вирішення інженерних і наукових завдань, які виникають під час розробки та дослідження механізмів.

Програму навчальної дисципліни розроблено відповідно 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. Робоча програма навчальної дисципліни відповідає вимогам державного стандарту освіти з напряму підготовки "Комп'ютерні науки".

2. Тематичний план навчальної дисципліни

При вивченні дисципліни "Захист інформації в інформаційних системах" студент має ознайомитися з програмою дисципліни, її структурою, формами та методами навчання, видами і методами контролю знань. Тематичний план дисципліни "Захист інформації в інформаційних системах" складається з одного модулю, який охоплює основні положення та механізми захисту інформації в інформаційних системах.

Навчальний процес здійснюється в таких формах: лекційні та лабораторні заняття, індивідуальна навчально-дослідне завдання, самостійна робота студента. Структура залікового кредиту навчальної дисципліни наведена в табл. 2.

Таблиця 2

Структура залікового кредиту навчальної дисципліни

Тема дисципліни	Кількість годин, відведених на:				
	лекції	лабораторні заняття	практичні заняття	самостійну роботу	ІНДЗ
1	2	3	4	5	6
Змістовний модуль 1. Політика безпеки, механізми та протоколи забезпечення захисту інформації в інформаційних системах					
Тема 1. Основи захисту інформації та життєвий цикл розробки систем безпеки	2			10	1

Закінчення табл. 2

1	2	3	4	5	6
Тема 2. Національні й міжнародні стандарти криптографічного захисту інформації в ІС	2			5	1
Тема 3. Криптографічні механізми захисту інформації в інформаційних системах	4	22		25	6
Тема 4. Комплексні системи захисту в корпоративних ІС	2	8		18	2
Усього	**10**	**30**		**58**	**10**

3. Зміст дисципліни за модулями та темами

Змістовний модуль 1. Політика безпеки, механізми та протоколи забезпечення захисту інформації в інформаційних системах

Тема 1. Основи захисту інформації та життєвий цикл розробки систем безпеки

Роль інформації в сучасному світі, значення захисту. Основні поняття та визначення. Критична, конфіденційна, особиста, державна інформація. Державна таємниця. Роль захисту інформації в ІС. Аналіз основних видів атак, ризиків і вразливих елементів інформаційних систем. Вимоги щодо безпеки системи, ризики безпеки. Послуги безпеки: конфіденційність, цілісність, доступність, причетність, спостереженість. Розподіл послуг безпеки за рівнями моделі ISO/OSI. Документ політика безпеки в інформаційних системах. Критерії захищеності комп'ютерних систем. Розробка профілю захисту. Механізми реалізації послуг безпеки. Стандарт ISO 7498-2. Побудова та впровадження систем захисту інформації.

Тема 2. Національні й міжнародні стандарти криптографічного захисту інформації в ІС

Міжнародні стандарти криптографічних методів захисту інформації. Стандарти безпеки банківської справи. Стандарти шифрування ANSI. Стандарти безпеки банківської справи ANSI. Міжнародні стандарти стосовно засад безпеки інформації й архітектурі безпеки. Урядові стандарти США (FIPS). Державні стандарти колишнього СРСР, Російської федерації (ГОСТ) та нормативно правові документи. Державні стандарти України (ДСТУ) й інші та нормативно правові документи. Запити коментарів (Request for Comments, RFC). Стандарти науково-дослідницьких і промислових організацій: IEEE, ITU-T, PKCS. Стандарти безпеки НАТО. Галузеві стандарти.

Тема 3. Криптографічні механізми захисту інформації в інформаційних системах

Компоненти криптосистеми та їх функціональні характеристики. Перестановка та підстановка. Прості шифри. Симетричне шифрування. Блочні симетричні шифри. Архітектура блочних симетричних шифрів. Характеристики і параметри сучасних блочних симетричних шифрів. Режими шифрування: "Електронна кодова книга", "Зчеплення блоків шифру", "Зворотний зв'язок по шифру", "Зворотний зв'язок по виходу". Режим простої заміни. Режим гама шифрування. Режим шифрування зворотним зв'язком за виходим. Режим вироблення імітовставки. Автентифікація та імітозахист інформації. Потокові шифри. Сфера застосування симетричних алгоритмів і режимів шифрування. Односпрямовані функції. Функція гешування. Важкозворотні функції, їх класифікація, еліптичні криві. Асиметричні криптоперетворення. Стійкість асиметричних криптоперетворень. Компоненти асиметричної системи. Генерування ключів. Загальносистемні параметри. Спрямоване шифрування та цифровий підпис. Загрози й атаки на цифровий підпис. Формування та перевірка цифрового підпису. Стандарти спрямованого шифрування і цифрового підпису. ДСТУ 4145. Алгоритми ЦП: RSA, Ель Гамаля (EGSA), ECDSA. Протоколи керування ключами. Протокол Дефі–Хелмана. Напрямки стеганографії. Класифікація систем цифрової стеганографії та їх використання. Стеганографія з відкритим ключем. Атаки на стегасистеми та протидія їм.

Тема 4. Комплексні системи захисту в корпоративних ІС

Визначення і класифікація задач курування доступом до ресурсів. Поняття "держатель" та "власник" інформації. Класифікація суб'єктів і об'єктів доступу. Модель управління доступом. Типи порушників. Класифікація мережних загроз та атак. Захист інформації за рівнями ISO\OSI. Фільтрація трафіка. Захист інформації за допомогою міжмережних екранів. Захист інформації на мережному рівні. Протоколи IPSec, SSL, TLS, їх сутність. Захищена електронна пошта. Архітектура та основні вимоги. Система PGP. Криптографічні функції. Сумісність на рівні електронної пошти. Захищена електронна пошта. Компоненти та сервіси інфраструктури відкритих ключів. Архітектура і топологія PKI. Стандарти в галузі PKI. Сертифікати відкритих ключів X.509. Системи PKI. Документ політика захисту інформації, його сутність і структура. Профілі безпеки автоматизованих систем. Основні вимоги до політиці PKI.

4. Плани лекцій

Змістовний модуль 1. Політика безпеки, механізми та протоколи забезпечення захисту інформації в інформаційних системах

Тема 1. Основи захисту інформації та життєвий цикл розробки систем безпеки

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

1.2. Роль інформації в сучасному світі. Основні поняття та визначення. Конфіденційна інформація. Законодавство в галузі захисту інформації.

1.3. Архітектура безпеки. Послуги безпеки. Принципи проектування систем захисту інформації.

1.4. Послуги безпеки. Критерії захищеності інформації в інформаційних системах. Профіль захищеності.

Література: основна [1; 3; 5; 6]; додаткова [9 – 11].

Тема 2. Національні й міжнародні стандарти криптографічного захисту інформації в ІС

2.1. Міжнародні стандарти криптографічних методів захисту інформації.

2.2. Державні стандарти України з методів захисту інформації.

2.3. Стандарти науково-дослідницьких і промислових організацій.

Література: основна [1; 3; 5; 7]; додаткова [9 – 11].

Тема 3. Криптографічні механізми захисту інформації в інформаційних системах

3.1. *Симетричні криптографічні системи шифрування.* Конфіденційність інформації. Класифікація симетричних шифрів. Вимоги до симетричних шифрів. Структура блочних симетричних шифрів. Національний стандарт блочного шифру.

3.2. Сучасні асиметричні шифри. Важкоборотні функції. Схема асиметричного шифрування. Компоненти асиметричної криптосистеми. Криптосистема RSA. Національний стандарт асиметричного шифрування.

3.3. Автентифікація інформації. Вимоги автентифікації. Односпрямовані геш-функції. MAC-коди. Характеристика алгоритмів MD5, SHA-1, HMAC.

3.4. Цифровий підпис. Вимоги до цифрового підпису. Правові аспекти використання цифрового підпису. ЦП Ель Гамаля. Національній стандарт цифрового підпису. Сумісний, груповий, арбітражний, довірений та сліпий підпис.

3.5. Протоколи керування ключами. Протокол Діффі – Хеллмана.

3.6. Цифрова стеганографія. Стеганографічні протоколи. Цифрові водяні знаки. Атаки на стегасистеми. Приховування даних у аудіосигналах та відеопослідовностях.

Література: основна [1; 3 – 6]; додаткова [10].

Тема 4. Комплексні системи захисту в корпоративних ІС

4.1. Модель управління доступом. Визначення і класифікація задач, вирішуваних механізмами управління доступом до ресурсів. Вимоги до механізмів управління доступом до ресурсів.

4.2. Основи мережної безпеки. Захист інформації за допомогою мережних екранів.

4.3. Захист інформації на мережному рівні. Протоколи IPSec, SSL, TLS, їх сутність.

4.4. Структура, сервіси й архітектура PKI. Стандарти і специфікації PKI. Принципи функціонування PKI.

4.5. Закон об інформації. Електроні документи та їх правовий статус. Служба захисту інформації.

4.6. Політика захисту інформації. Визначення цілей політики захисту інформації. Розробка документа політики захисту інформації підприємства.

Література: основна [1 – 5; 7]; додаткова [9; 10].

5. Плани лабораторних занять

Лабораторні заняття – форма навчального заняття, при 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 і 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 і практичних засобів вирішення 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 цілі повинні бути щільно зв’язані з практичними завданнями підготовки студента як фахівця.

Лабораторні заняття служать відбиттям принципів певних наукових шкіл, які склалися в університеті. В 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 в складі навчальної групи, яка об’єднує студентів з однаковою спеціальністю і спеціалізацією підготовки, на них вдається глибше пов’язати теорію з практикою в контексті майбутньої професійної діяльності фахівця й тим самим успішно реалізувати суб’єктно-діяльнісний підхід у навчанні.

Для успішної реалізації призначення і ролі лабораторних занять в структурі навчальної дисципліни та 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* відносяться:

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, щоб 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 повинне реалізовувати суб’єктно-діяльніс-ний (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 залежно 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 коригувати, уточнювати та поглиблювати знання студентів.

4. Основу лабораторного заняття має складати індивідуальна самостійна робота студентів при керуючому впливі викладача в сполученні із колективним обговоренням проблемних питань, відпрацюванням шляхів і методики розв’язання поставлених задач. Для підвищення ефективності індивідуальної роботи студентів, розвитку їх самостійності, доцільно передбачати й використати можливість

соціальної стимуляції з боку товаришів навчальної групи, створюючи тим самим обстановку відповідальної залежності кожного від колективу.

Специфічні вимоги до лабораторних занять характеризуватися 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 умінь, які наведені в освітньо-кваліфікаційній характеристиці випускника університету і забезпечуються дисципліною, що вивчається. Передбачати також формування певних знань і умінь, необхідних для освоєння відповідних спеціальних дисциплін. Зміст лабораторного заняття повинен визначатись диференційовано для кожної навчальної групи з урахуванням спеціальності (спеціалізації) підготовки студентів у 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 по *спеціальним дисциплінам* необхідно передбачати:

формування у студентів умінь 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 залежно від характеру дисциплін та курсу навчання. Тому стосовно структури можна дати тільки загальні рекомендації.

Кожне заняття повинно починатися зі вступу, в якому оголошується тема, цільова настанова і план проведення заняття. Визначається місце

заняття в навчальному процесі, називаються питання, які повинні бути засвоєні студентами при підготовці до заняття.

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

Виконання лабораторної роботи оцінюється викладачем. Підсумкова оцінка виставляється в 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 у табл. 3.

Таблиця 3

Перелік тем лабораторних занять

№ з/п	Теми лабораторних занять	Кількість годин
1.	Класичні симетричні системи. Дослідження крипостійкості простих симетричних шифрів	4
2.	Дослідження сучасних блочних симетричних шифрів та режимів шифрування	4
3.	Дослідження сучасних асиметричних криптосистем шифрування. Стандарт ДСТУ ISO\IEC 15948-3.	4
4.	Дослідження електроного цифрового підпису. ЦП Ель Гамаля, ДСТУ-4145, ECDSA	4
5.	Стеганографічні методи захисту інформації	4
6.	Аудит парольного захисту інформації	
7.	Безпечність персональних конфіденціальних даних на базі секретного диску та захищеної електронної пошти PGP	6
8.	Розгортання та управління інфраструктурою відкритих ключів	4

При проведенні ЛР студент повинен продемонструвати:

творчий підхід до дослідження тематики процедур і 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) з описом і поясненнями до використовуваного додатка.

Виконання ЛР містить такі етапи:

1. Підготовчий етап (до проведення ЛР):

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

б) вивчення теоретичного матеріалу за темою ЛР;

в) розробка алгоритму виконання завдання.

2. Безпосереднє виконання завдання в комп'ютерному класі обчислювального центра:

а) проходження допуску до ЛР;

б) установка (з потреби), конфігурування додатка;

в) відпрацьовування завдання за варіантом;

г) аналіз отриманих параметрів і характеристик.

3. Виконання звіту і захист ЛР.

Звіт з ЛР повинен містити:

титульний лист із найменуванням ЛР і даними виконавця;

дату виконання;

особистий підпис;

мету роботи;

опис завдання;

опис алгоритму виконання завдання;

результати роботи та їхній аналіз;

висновки з роботи.

Усі матеріали звіту необхідно зброшурувати, сторінки пронумерувати.

Звіт з ЛР згідно з нормативними актами повинен захищатися виконавцем. Форму проведення захисту ЛР обирає викладач.

6. Індивідуальне навчально-дослідне завдання

Індивідуальне навчально-дослідне завдання (ІНДЗ) виконується самостійно при консультуванні викладачем протягом вивчення дисципліни відповідно до графіка навчального процесу.

ІНДЗ виконується з метою систематизації закріплення, поглиблення і узагальнення знань, одержаних студентами за час навчання та придбання практичних навичок їх застосування при розв'язанні завдань забезпечення необхідного рівня захисту інформації в інформаційних системах на підприємстві.

Індивідуальне навчально-дослідне завдання припускає наявність наступних елементів наукового дослідження: практичної сутності; комплексного системного підходу до вирішення завдань дослідження; теоретичного використання передової сучасної методології і наукових розробок; наявність елементів творчості.

Практична сутність ІНДЗ полягає в обґрунтовуванні реальності його результатів для потреб практики.

Реальною вважається робота, яка виконана відповідно до наявних проблем підприємства, на основі його реальних даних з обробки інформації, і результати якої повністю або частково можуть бути впроваджені в практику діяльності підприємства або аналогічних об'єктів щодо забезпечення захисту інформації.

Комплексний системний підхід до розкриття теми роботи полягає в тому, що предмет дослідження розглядається під різними точками зору – з позицій теоретичної бази і практичних напрацювань, умов його реалізації, аналізу, обґрунтовування шляхів удосконалення механізмів та протоколів захисту інформації та ін. – в тісному взаємозв'язку і єдиній логіці викладу.

Застосування сучасної методології полягає в тому, що при виконанні дослідження показників роботи мережі підприємства і обґрунтовуванні шляхів удосконалення системи захисту інформації студент повинен використовувати відомості про новітні механізми та протоколи забезпечення необхідного рівня захисту.

У процесі виконання ІНДЗ, разом з теоретичними знаннями і практичними навиками за фахом, студент повинен продемонструвати здібності до науково-дослідної роботи і вміння творчо мислити, навчитися вирішувати науково-технічні задачі.

6.1. Тематика ІНДЗ

1. Секретність системи шифрування. Довершена секретність. Ентропія і невизначеність. Інтенсивність і надмірність язика. Відстань єдності й ідеальна секретність.

2. Класичні симетричні криптосистеми. Основні поняття і визначення. Шифри перестановки. Шифруючі таблиці. Застосування магічних квадратів тощо.

3. Класичні симетричні криптосистеми. Шифри простої заміни. Система шифрування Цезаря. Афінна система підстановок Цезаря. Система Цезаря з ключовим словом. Шифруючі таблиці Трісемуса. Біграмний шифр Плейфейра. Криптосистема Хілла.

4. Класичні симетричні криптосистеми. Шифри складної заміни. Система шифрування Віжінера. Шифр "подвійний квадрат" Уїтстона. Одноразова система шифрування. Шифрування методом Вернама.

5. Класичні симетричні криптосистеми. Шифрування методом гамірованія. Методи генерації псевдовипадкових послідовностей чисел.

6. Сучасні симетричні криптосистеми. Американський стандарт шифрування даних DES. Основні режими роботи. Режим "Електронна кодова книга". Режим "Зчеплення блоків шифру". Режим "Зворотний зв’язок по шифру". Режим "Зворотний зв’язок по виходу". Області застосування алгоритму DES. Криптоаналіз.

7. Сучасні симетричні криптосистеми. Комбінування блокових алгоритмів. Алгоритм шифрування даних IDEA. Криптоаналіз.

8. Сучасні симетричні криптосистеми. Стандарт шифрування даних ГОСТ 28147-89. Режим простої заміни. Режим вибірки гами. Режим шифрування зі зворотним зв’язком. Режим вироблення імітовставки.

9. Сучасні симетричні криптосистеми. Потокові шифри. Генератори псевдовипадкових послідовностей.

10. Сучасні симетричні криптосистеми. Алгоритм RC-4. Опис криптосхеми. Криптоаналіз.

11. Сучасні асиметричні криптосистеми. Концепція криптосистеми з відкритим ключем. Односпрямовані функції. Криптосистема шифрування даних RSA. Процедури шифрування і розшифрування в криптосистемі RSA. Безпека і швидкодія криптосистеми RSA. Криптоаналіз.

12. Сучасні асиметричні криптосистеми. Схема шифрування Діффі-Хеллмана.

13. Сучасні асиметричні криптосистеми. Схема шифрування Ель Гамаля.

14. Сучасні асиметричні криптосистеми. Комбінований метод шифрування.

15. Ідентифікація і перевірка достовірності. Основні поняття і концепції. Ідентифікація й автентифікація користувача. Типові схеми ідентифікації і автентифікації користувача. Особливості застосування пароля для автентифікації користувача. Біометрична ідентифікація і автентифікація.

16. Ідентифікація та перевірка достовірності. Взаємна перевірка достовірності користувачів. Протоколи ідентифікації з нульовою передачею знань. Спрощена схема ідентифікації з нульовою передачею знань. Паралельна схема ідентифікації з нульовою передачею знань. Схема ідентифікації Гиллоу-Куїськуотера.

17. Електронний цифровий підпис. Проблема автентифікації даних і електронний цифровий підпис. Односпрямовані геш-функції. Односпрямовані геш-функції на основі симетричних блокових алгоритмів. Вітчизняний стандарт геш-функції.

18. Електронний цифровий підпис. Алгоритми електронного цифрового підпису. Алгоритм цифрового підпису RSA. Алгоритм цифрового підпису Ель Гамаля (EGSA). Алгоритм цифрового підпису DSA. Вітчизняний стандарт цифрового підпису.

19. Електронний цифровий підпис. Цифрові підписи з додатковими функціональними можливостями. Схема сліпого цифрового підпису. Схема незаперечного цифрового підпису.

20. Управління криптографічними ключами. Генерація ключів. Зберігання ключів. Носії ключової інформації. Концепція ієрархії ключів.

21. Управління криптографічними ключами. Розподіл ключів. Розподіл ключів за участю центру розподілу ключів. Прямий обмін ключами між користувачами.

22. Додатки автентифікації. Система Kerberos. Діалоги автентифікації. Додатки автентифікації. Служба автентифікації X.509. Формати X.509. Процедура автентифікації X.509.

23. Безпека інформації в мережі INTERNET. Типові сервіси та комерційні вимоги щодо безпеки інформації в мережі INTERNET. Основні принципи забезпечення безпеки в мережі INTERNET.

24. Захист інформації в мережі INTERNET за допомогою брандмауерів.

25. Захист інформації на мережному рівні. Протокол IPsec.

26. Протокол SSL, його сутність. Специфікація протоколу. Основні компоненти. Протокол TLS, його сутність. Криптографічні алгоритми, що використовуються в SSL та TLS.

27. Захищена електронна пошта. Архітектура і основні вимоги. Система PGP. Криптографічні функції. Сумісність на рівні електронної пошти.

28. Захищена електронна пошта. Система S/MIME. Функціональні можливості S/MIME. Криптографічні алгоритми, використовувані в системі S/MIME. Повідомлення S/MIME.

29. Операційні системи. Уразливість операційних систем. Файлова система. Робочі групи та домени.

30. Методи приховування каналу передачі конфіденціальної інформації. Методи стеганографії.

6.2. Вимоги до змісту ІНДЗ

ІНДЗ виконується студентом самостійно. Студент має надати ІНДЗ для перевірки наприкінці семестру, але не пізніше терміну проведення підсумкового модульного контролю. Оцінка за виконання ІНДЗ враховується при виставленні загальної оцінки з дисципліни.

ІНДЗ складається з двох частин: теоретичної та практичної.

Тематика теоретичної частини ІНДЗ повинна носити проблемний характер. Студент має право самостійно обрати тему та зміст роботи з обов’язковим її узгодженням з викладачем.

У протилежному випадку тема має бути запропонована викладачем (варіанти тем наведені вище).

У процесі виконання ІНДЗ студент має опрацювати не менш п’яти літературних джерел з посиланнями на використання певної інформації з них у тексті роботи.

При цьому робота має носити творчий характер і бути спрямованою на вирішення певної проблеми чи на висловлення особистого погляду автора роботи на питання, яке розглядається в роботі.

Індивідуальне завдання складається з: титульної сторінки; змісту; вступу; основної частини; висновків; списку літератури, додатків до індивідуального завдання (з потреби).

Титульна сторінка. Повинна містити назву університету; назву кафедри; назву навчальної дисципліни; тему ІНДЗ з вказівкою бази дослідження; прізвище, ініціали студента, навчальна дисципліна, номер академічної групи; дату подання ІНДЗ викладачу на перевірку (день, місяць, рік), особистий підпис студента.

Зміст. Повинен відтворювати назви розділів, параграфів тощо, які розкривають тему ІНДЗ, із зазначенням номерів сторінок, на яких вони розміщені.

Вступ. У вступі студентом розкривається актуальність теми ІНДЗ та основні завдання для розробки теми ІНДЗ.

Основна частина. Складається з 3-х розділів.

Перший розділ повинен містити постановку задачі – необхідну і достатню сукупність відомостей щодо конкретної задачі захисту інформації; оцінки їх продуктивності та визначення рекомендацій для подальшого удосконалення, які визначають її сутність.

У цьому розділі студент повинен визначити:

1) характеристику задачі – призначення задачі, перелік об’єктів для яких вирішується задача; зв’язки з іншими механізмами та процедурами системи захисту інформації; призначення, місце та роль механізму або протоколу забезпечення захист інформації в ІС;

2) загальні повідомлення – перелік і опис вхідних та вихідних даних, принципи формування та розшифрування інформації, основні показники стійкості до зламування.

Другий розділ має містити інформацію щодо опису алгоритмів криптографічного перетворення та обробки інформації, який включає: призначення і математичний опис алгоритмів механізмів захисту інформації. Основні характеристики в табличному або графічному вигляді.

Третій розділ повинен містити результати досліджень порівняльних характеристик дослідного механізму (процедури або протоколу) з іншими.

Висновки. У висновках викладають перелік практичних рекомендацій щодо застосування механізму захисту інформації та результати одержані в ІНДЗ.

Список літератури. Джерела розміщувати слід у списку в алфавітному порядку прізвищ перших авторів або заголовків. Відомості

про джерела, які включені до списку, необхідно давати згідно з вимогами державного стандарту з обов’язковим наведенням праць.

Додатки. У додатки можуть бути включені матеріали, що є копією вхідних документів, звітів, або відеокадри, схеми алгоритму. При наявності кількох додатків оформлюється окрема сторінка "ДОДАТКИ", номер якої є останнім, що відноситься до обсягу ІНДЗ.

7. 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 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 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 в 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 і понять з галузі захисту інформації в ІС.

4. Підготовка до семінарських і практичних занять, дискусій, роботи в малих групах.

5. Підготовка до підсумкового контролю.

6. Контрольна перевірка в кожного студента особистих знань за питаннями для самостійного поглибленого вивчення та самоконтролю.

7. Робота над ІНДЗ.

Самостійна робота студентів проводиться з метою:

відпрацювання та засвоєння навчального матеріалу, закріплення й поглиблення знань, умінь і 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 в пошуку та набутті знань.

Без систематичної, безперервної самостійної роботи студентів протягом усього 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.

Професорсько-викладацький склад при проведенні різних видів занять:

подає рекомендації з методики вивчення дисциплін та окремих питань;

видає завдання на самостійну роботу і контролює їх виконання;

застосовує такі методичні прийоми викладання навчального матеріалу, які орієнтують студентів на роботу з літературою та самостійне здобування знань;

турбується про те, щоб видані завдання відповідали фактичному часу, який мають студенти;

аналізує та узагальнює досвід самостійної роботи студентів із вивчення матеріалу своєї дисципліни і вносить корективи в завдання.

На кафедрах доцільно розроблювати та видавати, особливо студентам, методичні рекомендації щодо вивчення навчальних дисциплін.

7.1. Питання для самостійного опрацювання

Змістовний модуль 1. Політика безпеки, механізми та протоколи забезпечення захисту інформації в інформаційних системах

Тема 1. Основи захисту інформації та життєвий цикл розробки систем безпеки

Питання для самостійного поглибленого вивчення

1. Державна таємниця. Критична та конфіденційна інформація.
2. Інтелектуальна власність. Електронні документи.
3. Концепція архітектурних засобів безпеки ISO.
4. Послуги безпеки. Їх розподіл за моделлю ISO.
5. Керування безпекою.
6. Функціональні вимоги безпеки.
7. Критерії адекватності систем безпеки. Профіль захисту.
8. Автентифікація джерела даних та об’єкта комунікацій.
9. Конфіденційність з’єднання, трафіка, віддаленого поля даних.
10. Цілісність з’єднання з відновленням.
11. Профіль безпеки.

Теми рефератів

1. "Оранжева книга"
2. Принципи побудови системи захисту інформації.
3. Проект профілю безпеки.

Література: основна [1; 3; 5; 6]; додаткова [9 – 11].

Тема 2. Національні й міжнародні стандарти криптографічного захисту інформації в ІС

Питання для самостійного поглибленого вивчення

1. Інформація як інтелектуальна власність.
2. Сертифікація засобів захисту інформації.
3. Електроні документи та електронний документообіг.

4. Стандарти безпеки банківської справи.
5. Стандарти в галузі інформаційної безпеки.
6. Міжнародні стандарти криптографічного захисту інформації.

Теми рефератів

1. Напрямки розвитку стандартів із захисту інформації в Україні.
2. Міжнародні стандарти криптографічного захисту.
3. Стандарти інформаційної безпеки НАТО.

Література: основна [1; 3; 5; 6]; додаткова [9 – 11].

Тема 3. Сучасні механізми та протоколи забезпечення захисту інформації в інформаційних системах

Питання для самостійного поглибленого вивчення

1. Механізми забезпечення конфіденційності на основі сучасних симетричних алгоритмів шифрування.
2. Принципи блочного шифрування.
3. Поняття секретності системи шифрування. Досконала секретність.
4. Ентропія і невизначеність. Інтенсивність й надмірність мови.
5. Відстань єдності та ідеальна секретність.
6. Режими роботи блочних шифрів.
7. Розподіл ключів. Сценарії розподілу ключів. Управління ключами.
8. Криптоаналіз симетричних сучасних схем шифрування.
9. Принципи побудови криптосистем з відкритим ключем.
10. Умови застосування методів криптографії з відкритим ключем.
11. Захищеність та обчислювальні аспекти алгоритму RSA.
12. Криптографічні перетворення на еліптичних кривих.
13. Механізми забезпечення автентичності на основі сучасних асиметричних процедур шифрування, MAC-кодів.
14. Сучасні алгоритми хешування.
15. Автентифікації повідомлень і геш-функція хешування.

16. Прості функції хешування. Захист функцій хешування.

17. Цифрові підписи і протоколи автентифікації.

18. Стандарти цифрового підпису.

19. Розподіл ключів за допомогою системи з відкритим ключем.

20. Національні стандарти криптографічного захисту ДСТУ-4145 та ISO/IEC 15946.

Теми рефератів

1. Принципи побудови та застосування блочних шифрів.

2. Принципи застосування асиметричних схем шифрування.

3. Механізми та засоби реалізації послуг конфіденційності та автентичності.

4. Механізми та засоби реалізації послуг цілісності, причетності та автентичності.

Література: основна [1; 3 – 6]; додаткова [10].

Тема 4. Комплексні системи захисту в корпоративних ІС

Питання для самостійного поглибленого вивчення

1. Механізми та служби автентифікації системи Kerberos.

2. Методи шифрування. Розподіл ключів у системі Kerberos.

3. Механізми та протоколи захисту електронної пошти PGP.

4. Алгоритми стиснення інформації.

5. Алгоритми декомпресії. Перетворення в формат radix-64.

6. Захист інформації на рівні IP. Архітектура захисту. Сервіс IPSec.

7. Протоколи захисту прикладного рівня.

8. Поняття захищеного зв’язку. Тунельний та транспортний режими.

9. Протоколи міжмережної взаємодії.

10. Принципи побудови PKI.

11. Протоколи SSL і TLS.

12. Принципи розробки та застосування брандмауерів.

13. Загальні принципи побудови системи захисту інформації.

14. Система сертифікації. Сертифікати X.509

15. Основні правила захисту. Склад та призначення основних підсистем захисту інформації.

16. Методи та протоколи захисту інформації на різних рівнях еталонної системи взаємодії відкритих систем.

Теми рефератів

1. Захист інформації в мережі Internet.
2. Система автентифікації Kerberos
3. Механізми і протоколи захисту електронної пошти PGP.

Література: основна [2; 3; 6 – 8]; додаткова [9; 10].

7.2. Тематика контрольних робіт для студентів заочної форми навчання

Контрольна робота є однією з форм контролю та обліку знань і 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, будучи, в основному, засобом контролю, в той же час виконує навчальні та виховні функції. Контрольні роботи проводяться, як правило, в 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 завідувачем кафедри.

Лектор потоку у вступній лекції по дисципліні 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 номера в журналі.

Варіанти задач до контрольних робіт

Варіант 1

1. Класифікація інформації:
   а) поняття конфіденційна інформація;
   б) грифи таємності та терміни їх дії.
2. Симетричне шифрування:
   а) архітектура блочних симетричних шифрів;
   б) режим шифрування "зчеплення блоків шифру".
3. Мережна безпека трафіка:

а) режими протоколу IPEC;
б) протоколи безпеки трафіку на прикладному рівні.

Варіант 2

1. Європейські стандарти криптографічного захисту:
   а) стандарти цифрового підпису;
   б) стандарти керування безпекою.
2. Криптографічні методи реалізації конфіденційності:
   а) описати процес спрямованого шифрування;
   б) режим шифрування "зворотній зв’язок по виходу".
3. Керування доступом до ресурсів:
   а) поняття "держатель" та "власник" інформації;
   б) модель управління доступом.

Варіант 3

1. Архітектура безпеки:
   а) сутність послуги безпеки спостережності;
   б) сутність послуги безпеки цілісності.
2. Автентифікація повідомлень:
   а) поняття автентифікації;
   б) алгоритми автентифікації.
3. Система PGP:
   а) архітектура систем PGP;
   б) архітектура захищеної електродної пошти.

Варіант 4

1. Національні стандарти:
   а) державні стандарти цифрового підпису;
   б) державні стандарти управління безпекою.
2. Мережна безпека:
   а) класифікація мережних атак та загроз;
   б) поясніть принцип фільтрації трафіку.
3. Цифровий підпис:
   а) поняття цифрового підпису;
   б) архітектура цифрового підпису.

Варіант 5

1. Архітектура безпеки:
   а) сутність послуги безпеки конфіденційність;
   б) сутність послуги безпеки доступність.
2. Асиметрична криптографія:
   а) важкозворотні функції та їх класифікація;
   б) протоколи керування ключами.
3. Інфраструктура відкритих ключів:
   а) компоненти інфраструктури відкритих ключів;
   б) архітектура PKI.

8. Контрольні запитання для самодіагностики

Змістовний модуль 1. Політика безпеки, механізми та протоколи забезпечення захисту інформації в інформаційних системах

Тема 1. Основи захисту інформації та життєвий цикл розробки систем безпеки

1. Сутність інформації як матеріальної цінності.
2. Конфіденційна інформація.
3. Державна таємниця. Грифи таємності.
4. Інтелектуальна власність.
5. Правовий статус електронного документа.
6. Послуги безпеки.
7. Норми законодавства з питань захисту інформації.
8. Архітектура системи захисту інформації.
9. Політика безпеки інформаційної системи.
10. Критерії захищеності інформаційної системи.
11. Погрози та ризики безпеки інформації.

Література: основна [1 – 6]; додаткова [9 – 11].

Тема 2. Національні й міжнародні стандарти криптографічного захисту інформації в ІС

Питання для самостійного поглибленого вивчення

1. Стандарти з надання послуги конфіденційності інформації.
2. Європейські стандарти безпеки банківської справи.
3. Стандарти захисту інформації НАТО.
4. Запити коментарів (Request for Comments, RFC) з захисту інформації.

Література: основна [1; 2; 4; 6]; додаткова [9 – 11].

Тема 3. Криптографічні механізми захисту інформації в інформаційних системах

1. Структура криптосистем.
2. Принципи симетричного шифрування.
3. Проведіть порівняльний аналіз режимів шифрування.
4. Опишіть структуру симетричних шифрів.
5. У чому полягають автентифікація повідомлень.
6. Сутність режиму гама-шифрування.
7. Дайте характеристику потовим шифрам.
8. Назвіть властивості односпрямованих функції.
9. Дайте визначення геш-функції, її властивості.
10. Назвіть властивості важкооборотних функцій.
11. Дайте визначення відкритого та особистого ключа.
12. Сутність криптографії з відкритим ключем.
13. Криптоперетворення на еліптичній кривій.
14. Опишіть загальний алгоритм спрямованого шифрування.
15. Алгоритм RSA та його стійкість.
16. У чому полягає сутність електронного цифрового підпису.
17. Опишіть загальний алгоритм електронного цифрового підпису.
18. Стандарт ДСТУ 4145.
19. Принципи приховування каналу передачі конфіденційної інформації.
20. Стеганографічні методи приховування інформації в графічних зображеннях.
21. Сутність стеганографії з відкритим ключем.
22. У чому полягає протидія відомим атакам на стегасистеми.

Література: основна [1; 3 – 6]; додаткова [10].

Тема 4. Комплексні системи захисту в корпоративних ІС

1. Навести класифікацію задач керування доступом до ресурсів.
2. Опишіть модель управління доступом.
3. Дайте визначення "держатель" та "власник" інформації.
4. Дайте визначення брандмауера.
5. Дайте визначення файервола.
6. Сутність фільтрації трафіка.
7. Принципи захисту інформації на мережному рівні. Протокол IPSec.
8. Принципи захисту інформації на прикладному рівні.
9. Опишіть сертифікат відкритих ключів X.509.
10. Поняття захищеного зв'язку. Тунельний і транспортний режими.
11. Архітектура і топологія PKI.

Література: основна [2; 5 – 8]; додаткова [9; 10].

9. Індивідуально-консультативна робота

Індивідуально-консультативні заняття (ІКЗ) – вид навчального заняття, при яких 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 і 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 в 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 в 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 у форму

натаскування 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 і 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.

10. Методики активізації процесу навчання

При викладанні дисципліни "Захист інформації в інформаційних системах" для активізації навчального процесу передбачено застосування сучасних навчальних технологій, таких як: проблемні лекції, роботи в малих групах, розігрування іграшкових ситуацій, "мозковий штурм". Розподіл форм та методів активізації процесу навчання за темами навчальної дисципліни наведений у табл. 4.

Таблиця 4

Розподіл форм та методів активізації процесу навчання за темами навчальної дисципліни

Тема	Практичне застосування навчальних технологій
1	2
ТЕМА 1. Основи захисту інформації та життєвий цикл розробки систем безпеки	*Проблемна лекція* "Визначення базових засад захисту інформації в інформаційної системі підприємства"

Закінчення табл. 4

1	2
ТЕМА 2. Національні й міжнародні стандарти криптографічного захисту інформації в ІС	Міні-лекція "Класифікація та огляд національних та міжнародних стандартів захисту інформації. Визначення перспективного напрямку гармонізації міжнародних стандартів"
ТЕМА 3. Криптографічні механізми захисту інформації в інформаційних системах	Кейс "Проведення криптоаналізу класичних шифрів". Міні-лекція "Методика визначення крипостійкості та дослідження основних характеристик симетричних та асиметричних криптосистем"
ТЕМА 4. Комплексні системи захисту в корпоративних ІС	*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 у 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 та змістом, створює можливості для участі кожного студента в роботі за темою заняття, забезпечує формування особистісних якостей та досвіду соціального спілкування.

Семінари-дискусії передбачають обмін думками і поглядами учасників з приводу даної теми, а також розвивають мислення, допомагають формувати погляди й переконання, виробляють вміння формулювати думки й висловлювати їх, вчать оцінювати пропозиції інших людей, критично підходити до власних поглядів.

Мозкові атаки – це метод розв'язання невідкладних завдань за дуже обмежений час. Сутність його полягає в тому, щоб висловити якнайбільшу кількість ідей за невеликий період часу, обговорити і здійснити їх селекцію.

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 в 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 усім присутнім брати участь у процесі вироблення рішень, відчуваючи при цьому свою повну відповідальність за результат.

11. Система поточного та підсумкового контролю знань студентів

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

Оцінювання знань, умінь і навичок студентів враховує види занять, які згідно з програмою навчальної дисципліни "Захист інформації в інформаційних системах" передбачають лекційні та лабораторні заняття, а також самостійну роботу й виконання індивідуальних завдань.

Перевірка та оцінювання знань студентів може проводитись кількома методами:

1. Оцінювання знань студента під час лабораторних занять.

2. Оцінювання виконання індивідуального навчально-дослідного завдання.

3. Написання рефератів.

4. Виконання завдань для самостійної роботи.

5. Проведення проміжного контролю.

6. Проведення модульного контролю.

7. Проведення підсумкового контролю.

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.

Загальна оцінка з дисципліни визначається як середнє арифметичне модульної оцінки та оцінки за результатами 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 індивідуального навчально-дослідного завдання;

3) виконання проміжного контролю;

4) виконання модульного контрольного завдання.

Контроль систематичного виконання самостійної роботи та активності на лабораторних заняттях

Оцінювання проводиться за 12-бальною шкалою за такими критеріями:

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

2) ступінь засвоєння фактичного матеріалу навчальної дисципліни;

3) знайомлення з рекомендованою літературою, а також із сучасною літературою з питань, що розглядаються;

4) уміння 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;

5) 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 чи 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). Якщо якась із вимог не буде виконана, то оцінка на розсуд викладача, буде знижена.

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

Реферат є додатковою частиною самостійної роботи студента над навчальною дисципліною "Захист інформації в інформаційних системах". Мета реферату – поглиблення теоретичних знань, набутих студентами в процесі вивчення дисципліни.

Написання реферату має сприяти глибшому засвоєнню студентами дисципліни "Захист інформації в інформаційних системах", спонукає ґрунтовно вивчати нормативно-законодавчу базу, статистичні матеріали, спеціальні наукові видання вітчизняних і закордонних авторів, у яких розглядаються питання впровадження та ефективного використання механізмів захисту інформації в інформаційних системах.

Першим етапом написання реферату є вибір теми. Студенти обирають тему реферату за власним розсудом, але відповідно до тематики рефератів, визначеної кафедрою інформаційних систем. За погодженням з викладачем студент може підготувати реферат на іншу тему, якої немає у цьому переліку.

Після вибору теми студент повинен розробити й вкласти в письмовій формі його план. План теми слід розробляти після ознайомлення з літературними джерелами, які висвітлюють ті чи інші питання і проблеми з теми дослідження.

План має включати лише ті питання, які безпосередньо стосуються теми і дають змогу повно та глибоко розкрити її.

Писати реферат слід на білих аркушах стандартного формату А4, які треба зшити будь-яким способом.

Титульний аркуш реферату повинен мати такий зміст: назва університету; назва кафедри; назва навчальної дисципліни; тема реферату; прізвище, ініціали студента, навчальна дисципліна, номер академічної групи; дата подання реферату викладачу на перевірку (день, місяць, рік), особистий підпис.

За титульним аркушем йде детальний план реферату, в якому треба виділити вступ, два – три підрозділи основного змісту, висновки та список використаної літератури, додатки.

Складні таблиці, які не вміщуються в тексті, а також інші допоміжні матеріали включаються в додатки до роботи. При цьому в тексті на них робляться відповідні посилання.

Усі аркуші слід пронумерувати – порядковий номер ставиться в правому верхньому куточку сторінки, при цьому нумерація починає ставиться на першому аркуші після вступу.

У кінці реферату дається повний список використаних джерел. Його необхідно скласти у певному порядку: спочатку наводяться законодавчі та нормативні акти, статистичні довідники, загальна та спеціальна література за алфавітом.

Реферат має бути виконано і подано на кафедру не пізніше зазначеної в навчальному плані дати.

Реферат оцінюється за критеріями:

самостійності виконання;

логічності та деталізації плану;

повноти й глибини розкриття теми;

наявності ілюстрації (таблиці, рисунки, схеми тощо);

кількості використаних джерел (не менше десяти);

використання цифрової інформації та відображення практичного досвіду;

наявність конкретних пропозицій і прогнозів з обов'язковим посиланням на використані літературні джерела;

якості оформлення.

Підготовка якісного реферату може бути додатковою умовою отримання студентом позитивної підсумкової оцінки з даної навчальної дисципліни.

Проміжний 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 й множинного вибору різного рівня складності. Для оцінювання рівня відповідей студентів на тестові завдання використовуються наступні критерії оцінювання:

оцінка "відмінно" (12 – 10 балів) – виставляться у випадку, якщо студент правильно відповів на 20 – 18 тестових запитань;

оцінка "дуже добре" (9 балів) – 17 – 16 правильних відповідей;

оцінка "добре" (8 – 7 балів) – 15 – 13 правильних відповідей;

оцінка "задовільно" (6 балів) – 12 – 10 правильних відповідей;

оцінка "достатньо" (5 – 4 балів) – 9 – 7 правильних відповідей;

оцінка "незадовільно" (3 бали) – 6 – 5 правильних відповідей;

оцінка "незадовільно" (2 – 1 бали) – 4 – 2 правильних відповідей.

Тести для проміжного контролю обираються із загального переліку тестів за відповідними модулями.

Метою вирішення тестових завдань з навчальної дисципліни "Захист інформації в інформаційних системах" є засвоєння студентами теоретичних знань з методів та процедур забезпечення захист інформації в ІС, придбання практичних вмінь та навичок у 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 та евристичних), згідно яких має здійснюватися підготовка фахівця певного рівня кваліфікації.

Критерії оцінювання індивідуального навчально-дослідного завдання

Індивідуальне навчально-дослідне завдання оцінюється за такими критеріями:

1) самостійність виконання;

2) логічність та послідовність викладення матеріалу;

3) повнота розкриття теми (проблемної ситуації чи практичного завдання);

4) обґрунтованість висновків;

5) використання статистичної інформації та додаткових літературних джерел;

6) наявність конкретних пропозицій;

7) якість оформлення.

Проведення поточно-модульного контролю

Поточно-модульний контроль здійснюється та оцінюється за двома складовими: практичний модульний контроль і лекційний (теоретичний) модульний контроль. Оцінка за практичну складову модульного контролю виставляється за результатами оцінювання знань студента під час лабораторних занять, виконання індивідуального завдання та проміжного тестового контролю згідно з графіком навчального процесу.

Лекційний модульний контроль здійснюється в письмовій формі за відповідними білетами або тестами. Структура білетів (тестів) з модульного контролю аналогічна структурі білетів (тестів) з письмового іспиту. Для підведення підсумків роботи студентів із змістовного модуля виставляється підсумкова оцінка з поточно-модульного контролю, яка враховує оцінки за практичний модульний контроль і лекційний модульний контроль.

Завдання модульного контролю містить 2 завдання з лекційного модуля та 2 завдання з практичного модуля (стереотипне та евристичне).

Зразок модульного завдання

Теоретична частина

1. Охарактеризувати основні види атак на інформаційні системи.
2. Алгоритм асиметричного шифрування RSA.

Практична частина

Завдання 1 (стереотипне). Навести приклади процедур забезпечення автентичності повідомлень.

Завдання 2 (евристичне).

Ви є користувачем розподіленої захищеної системи до якої входять 6 користувачів. У даній системі користувачі можуть здійснювати несиметричне шифрування (розшифрування) RSA і виробляти або перевіряти цифровий підпис RSA для передавання повідомлень.

Таблиця

Користувач	Параметр системи n		Ключі користувачів	
	p	**q**	Відкритий (публічний) **e**	Приватний (секретний) **d**
A	23	11	79	
B	19	13		85
C	11	19	37	
D	17	13		43
E	11	17	51	
F	17	19		61

Ви користувач "A".

Перевірити, що ваші ключі (відкритий і приватний) вибраний правильно.

Розшифруйте повідомлення M, отримане від користувача "F".

Таблиця

Формат повідомлення

Тип алгоритму	Відправник	Адресат	Повідомлення	Хеш-значення	ЦП
Шифрування RSA	F	A	133	–	–

Викладач _____

(підпис)

Проведення підсумкового контролю. Умовою допуску підсумкового контролю є позитивні оцінки з проміжного контролю знань. Підсумковий контроль знань студентів здійснюється у формі тестів за 12-бальною шкалою.

Тести включають такі завдання:

1) теоретичне запитання;
2) практичні завдання різного ступеня складності.

Кожне завдання тесту оцінюється окремо. Загальна оцінка дорівнює середній арифметичній із суми оцінок кожного завдання. Якщо одна з оцінок "незадовільно", то загальна оцінка не може бути вищою за "задовільно".

Для оцінки рівня відповідей студентів на теоретичні запитання та вирішення практичних завдань використовуються такі критерії:

оцінка **"відмінно"** (11–12 балів) ставиться за глибоке засвоєння програмного матеріалу, засвоєння рекомендованої літератури; чітке володіння понятійним апаратом, методами, методиками та інструментами організації архітектури комп'ютерів, вміння використовувати їх для виконання конкретних практичних завдань. Відповідь на теоретичне питання білета має бути правильною та повною, оформлення відповіді – акуратним, логічним та послідовним;

оцінка **"відмінно"** (10 балів) ставиться за повне засвоєння програмного матеріалу та рекомендованої літератури; чітке володіння понятійним апаратом, методами, методиками та інструментами організації архітектури комп'ютерів, вміння використовувати їх для виконання конкретних практичних завдань, розв'язання ситуацій. Відповідь на теоретичне питання білета має бути правильною та повною, оформлення відповіді – акуратним, логічним та послідовним. Припускаються незначні випадкові погрішності, які не надають суттєвого впливу на повноту та змістовність відповіді;

оцінка **"добре"** (8 – 9 балів) ставиться за повне засвоєння програмного матеріалу та наявне вміння орієнтуватися в ньому, усвідомлене застосування знань для розв'язання практичних задач. Оцінка "добре" ставиться за умови виконання всіх вимог, які передбачено для оцінки "відмінно", при наявності незначних помилок (тобто методичний підхід до вирішення задачі є правильним, але припущені неточності у розробленні певних питань з організації архітектури комп'ютерів) або не зовсім повних висновків по одержаних результатах вирішення задачі. Оформлення виконаного завдання має бути охайним;

оцінка **"задовільно"** (7 балів) ставиться за неповне висвітлення змісту теоретичних питань та недостатнє вміння застосовувати теоретичні

знання для розв’язання практичних задач. Оцінка "задовільно" ставиться за умови, якщо завдання в основному виконане та мету завдання досягнуто, а студент при відповіді продемонстрував розуміння основних положень матеріалу навчальної дисципліни;

оцінка **"достатньо"** (4 – 6 балів) ставиться за часткове висвітлення змісту теоретичних питань та часткове вміння застосовувати теоретичні знання для розв’язання практичних задач. Оцінка "достатньо" ставиться за умови, якщо завдання частково виконане, а студент при відповіді продемонстрував розуміння основних положень матеріалу навчальної дисципліни;

оцінка **"незадовільно"** (3 бали) ставиться за не опанування значної частини програмного матеріалу, невміння виконувати практичні завдання, розв’язувати задачі.

оцінка **"незадовільно"** (1 – 2 бали) ставиться за невиконання завдання загалом.

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. 5).

Для підведення підсумків роботи студентів з навчальної дисципліни "Захист інформації в інформаційних системах" виставляється загальна оцінка, яка враховує оцінки з кожного виду контролю (оцінку модульного контролю, за роботу протягом семестру та оцінку за результатами підсумкового контролю).

Підсумковою оцінкою з дисципліни "Захист інформації в інформаційних системах" є середня оцінка, що отримана між оцінками під час складання іспиту та оцінки, отриманою на підсумковому контролі.

Критерії оцінювання знань студентів під час складання іспиту наведені в табл. 6.

Таблиця 5

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

Відсоток студентів, які зазвичай успішно досягають відповідної оцінки	Оцінка за шкалою ECTS		Оцінка за бальною шкалою, що використовується в ХНЕУ	Оцінка за національною шкалою
1	2	3	4	5
10	відмінне виконання	A	12 – 11	відмінно
25	вище середнього рівня	B	10	
30	взагалі робота правильна, але з певною кількістю помилок	C	9 – 7	добре
25	непогано, але зі значною кількістю недоліків	D	6	задовільно

Закінчення табл. 5

1	2	3	4	5
10	виконання задовольняє мінімальні критерії	E	5 – 4	
–	Потрібне повторне перескладання	FX	3	незадовільно
–	повторне вивчання дисципліни	F	2 – 1	

Таблиця 6

Критерії оцінювання знань студентів

Кількість балів	Критерії
1	2
12	Вільно володіє понятійним апаратом за всіма розділам дисципліни, її основними концепціями, стандартами при вирішенні завдання, знає цілі, зміст завдань, розуміє й може пояснити логіку виконання завдання, має стійкі навички вирішення завдання
11	Вільно володіє понятійним апаратом за всіма розділами дисципліни, її основними концепціями, стандартами при вирішенні завдання, знає цілі, зміст завдань, розуміє логіку виконання завдання, має стійкі навички вирішення завдання
10	Вільно володіє понятійним апаратом за всіма розділами дисципліни, її основними концепціями, стандартами при рішенні завдання, знає цілі, зміст завдань, може пояснити послідовність виконання завдання, має стійкі навички вирішення завдання
9	Вільно володіє понятійним апаратом за даним розділом дисципліни, її основними концепціями, стандартами при вирішенні завдання, знає цілі, зміст завдань, хід виконання завдання, має навички вирішення завдання
8	Допускає деякі незбіжності в визначеннях і поняттях, знає стандарти для рішення завдання, знає цілі, хід виконання завдання, має навички для рішення завдання
7	Допускає незбіжності в поняттях, знає стандарти для вирішення завдання, знає цілі, хід виконання завдання, має навички вирішення окремих частин завдання
6	Знає стандарти для вирішення завдання, але не може коректно їх використовувати, допускає незбіжності в понятійному апараті, має представлення про деякі стандарти, мету, хід виконання завдання, має навички рішення окремих частин завдання, неправильно використовує теоретичні положення при вирішенні завдання
5	Має уявлення про деякі стандарти, мету, хід виконання завдання, має нестійкі навички вирішення окремих частин завдання, неправильно використовує теоретичні положення при вирішенні завдання
4	Має уявлення про деякі стандарти, мету, хід виконання завдання, недостатньо володіє термінологією, знає тільки частину визначень та понять, має нестійкі навички вирішення окремих частин завдання, при вирішенні завдання не показує знань теоретичних положень

Закінчення табл. 6

1	2
3	Не послідовне вирішення завдання, допущені помилки при вирішенні завдання, побудова матеріалу нелогічна, в термінах та поняттях допускаються помилки, які приховують їх зміст, не має представлення про мету та хід виконання завдання, не має навичок вирішення окремих частин завдання
2	Є систематичні помилки, які скривлюють зміст вирішення завдання, відсутнє представлення про стандарти та концепції при вирішенні завдання, не має уявлення про мету та хід виконання завдання, не має навичок вирішення окремих частин завдання
1	Усі відповіді на вирішення завдання неправильні, не має уявлення про мету та хід виконання завдання, не має навичок вирішення окремих частин завдання

Приклад запитань екзаменаційного тестового завдання

Завдання 1

Визначити (перестановочний, моноалфавітний або поліалфавітний) метод шифрування із переліку методів, якій наведено в п.1.1).

1.1. Методи шифрування:

Перестановки з ключовим словом.

Матричної перестановки.

Простої заміни.

Цезаря.

Цезаря з ключовим словом.

Плейфєра.

Віжинера.

З автоключем з використанням відкритого тексту.

З автоключем з використанням криптограми.

Поліалфавітний.

Завдання 2

Зашифрувати за допомогою визначеного в завданні 1 методу шифрування відкритий текст (див. п.2.1). Потрібний для шифрування ключ(і) наведено в п. 2.2. Алфавіт(и) наведено в п. 2.3.

2.1. Відкритий текст:

"*КРИТЕРІЇ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ*"

2.2. Ключ(і):

"*АЛГОРИТМ*"

2.3. Алфавіт(и):

Український алфавіт, літери вид "А" до "Б" з доданням пробілу " ".

Завдання 3

Визначити (перестановочний, моноалфавітний або поліалфавітний) метод шифрування із переліку методів, якій наведено в п. 3.1).

3.1. Методи шифрування:

Перестановки з ключовим словом.

Матричної перестановки.

Простої заміни.

Цезаря.

Цезаря з ключовим словом.

Плейфєра.

Віжинера.

З автоключем з використанням відкритого тексту.

З автоключем з використанням криптограми.

Поліалфавітний.

Завдання 4

Розшифрувати за допомогою визначеного у завданні 3 методу шифрування відкритий текст (див. п.4.1). Потрібний для шифрування ключ(и) і наведено в п. 4.2. Алфавіт(и) наведено в п. 4.3.

4.1. Криптограма:

"МЕХАНІЗМИ РЕАЛІЗАЦІЇ ПОСЛУГИ КОНФІДЕНЦІЙНОСТІ"

4.2. Ключ(і):

"ПРОТОКОЛ"

4.3. Алфавіт(и):

Український алфавіт, літери від "А" до "Б" з доданням пробілу " ".

Завдання 5

Для наведених у п.5.1. загроз інформаційної безпеки розрахувати рівні ризику та розташувати в порядку їхнього убування.

5.1. Загрози:

№ з/п	Загроза	Рівень збитку, у.о.	Ймовірність виникнення (здійснення), %
1			
2			
3			

Завдання 6

Для загрози з найбільшим рівнем ризику (див. завдання 5) запропонувати контрзаходи (методи та засоби захисту інформації), які мінімізують цей рівень ризику. Обґрунтувати вибір контрзаходів.

12. Рекомендована література

12.1. Основна

1. Емельянов С. П. Основы информационной безопасности: Конспект лекций. – Одесса: Юридична література, 2003. – 200 с.

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

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

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

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

6. Пономаренко В. С. Основи захисту інформації. Навчальний посібник / В. С. Пономаренко, І. В Журавльова. – Харків: Вид. ХДЕУ, 2003. – 176 с.

7. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М.: СОЛОН-Прес, 2002. – 272 с. (Серия "Аспекты защиты")

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

12.2. Додаткова

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

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

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

12.3. Ресурси мережі Internet

12. http://bezopasnost.biz.

13. http://dstszi.gov.ua.

14. Журнал "Информационные технологии. Аналитические материалы" // http://it.ridne.net

15. Центр информационных технологий. // http://www.citmgu.ru

16. Нормативные акты Украины // www.nau.kiev.ua

17. Information Technology Security Evaluation Criteria, v.1.2. -Office for Official publications of the European Communities, 1991.

18. www.fbi.gov.

19. www.pgpi.org.

20. www.rootshell.com.

21. www.securityfocus.com.

22. www.sysinternals.com.

23. www.zdnet.ru.

24. www.submarine.ru.

25. www.securitylab.ru.

Зміст

НАВЧАЛЬНЕ ВИДАННЯ

Робоча програма
навчальної дисципліни
"ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ"
для студентів напряму підготовки "Комп'ютерні науки"
денної форми навчання

Укладачі: **Євсеєв Сергій Петрович**
Огурцов Віталій Вячеславович
Поляков Андрій Олександрович

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

Редактор **Замазій О. Є.**

Коректор **Голінська О. Г.**

План 2008 р. Поз. №222.
Підп. до друку Формат 60 × 90 1/16. Папір MultiCopy. Друк Riso.
Ум.-друк. арк. 3,0. Обл.-вид. арк. 3,75. 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.***

Робоча програма

навчальної дисципліни

"ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ"

для студентів напряму підготовки "Комп'ютерні науки"

денної форми навчання