МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

Робоча програма
навчальної дисципліни

"ЗАХИСТ ІНФОРМАЦІЇ"

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

Харків
ХНЕУ ім. С. Кузнеця
2016

Затверджено на засіданні кафедри інформаційних систем.
Протокол № 1 від 27.08.2015 р.

Самостійне електронне текстове мережеве видання

Укладачі: С. П. Євсеєв
О. Г. Король

Робоча програма навчальної дисципліни "Захист інформації"
Р 58 для студентів напряму підготовки 6.050101 "Комп'ютерні науки" всіх форм навчання : [Електронне видання] / уклад. С. П. Євсеєв, О. Г. Король. – Харків : ХНЕУ ім. С. Кузнеця, 2016. – 50 с.

Подано тематичний план навчальної дисципліни та її зміст за модулями й темами. Вміщено плани лекцій та лабораторних занять, матеріали для закріплення знань (завдання для самостійної роботи, контрольні запитання), критерії оцінювання знань студентів, професійні компетентності, якими повинен володіти студент після вивчення дисципліни.

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

Вступ

Захист інформації перетворюється сьогодні на одне з найактуальніших завдань унаслідок надзвичайно широкого розповсюдження як власне різноманітних систем оброблення інформації, так і поширення локальних і глобальних комп'ютерних мереж, якими передаються величезні обсяги інформації державного, військового, комерційного, приватного характеру, власники якої часто були б категорично проти ознайомлення з нею сторонніх осіб. Проблема набуває особливої гостроти після ухвалення Урядом України закону про захист персональних даних, який зобов'язує зберігати та передавати персональні дані працівників лише в захищеному вигляді в інформаційних системах (ІС).

Не менш важливим завданням вважається широке впровадження інформаційних технологій у різні сфери людської діяльності в Україні: стрімке зростання обігу пластикових карток, майбутнє введення електронних паспортів і медичних карт, студентських квитків і залікових книжок; зрештою все більше державних установ і приватних підприємств переходять на електронний документообіг, який потребує юридичної чинності підпису фізичної або юридичної особи. Розповсюдження таких технологій, безперечно, вимагає добре організованого захисту інформації.

Навчальна дисципліна "Захист інформації" є базовою та вивчається згідно з навчальним планом підготовки фахівців першого освітнього ступеня "бакалавр" спеціальності 122 "Комп'ютерні науки та інформаційні технології" всіх форм навчання.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Показники</td><td rowspan="2">Галузь знань, спеціальність, освітній рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4</td><td>Галузь знань
12 "Комп'ютерні науки"</td><td colspan="2">Базова</td></tr>
<tr><td rowspan="8">Змістових модулів – 2</td><td rowspan="8">Спеціальність
122 "Комп'ютерні науки та інформаційні технології"</td><td colspan="2">Рік підготовки</td></tr>
<tr><td>4-й</td><td>5-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>8-й</td><td>9-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>20 год</td><td>20 год</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td rowspan="8">Тижневих годин для денної форми навчання:
аудиторних – 6;
самостійної роботи студента – 6</td><td rowspan="8">Перший освітній рівень: бакалавр</td><td colspan="2">Лабораторні</td></tr>
<tr><td>40 год</td><td>16 год</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>60 год</td><td>84 год</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td colspan="2">залік</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
</table>

Примітка. Співвідношення кількості годин аудиторних занять до самостійної й індивідуальної роботи становить:

для денної форми навчання – 50 %;

для заочної форми навчання – 70 %.

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни "Захист інформації" є навчання студентів принципам побудови комплексних систем захисту інформації, дослідженню та використанню сучасних процедур забезпечення надання основних послуг безпеки інформації в банківських системах, що засновані на використанні алгоритмів симетричної та несиметричної криптографії в комунікаційних системах, протоколів інфраструктури відкритих ключів (ІВК).

Для досягнення мети поставлені такі основні **завдання**:

аналіз основ теорії захисту інформації щодо системного підходу до організації комплексних систем захисту даних на основі застосування криптографічних методів;

дослідження сучасних протоколів і процедур щодо забезпечення основних послуг безпеки відповідно до стандартів ISO-7498-2, ISO/IEC 10181, 11770;

дослідження основних протоколів захисту інформації в банківських системах відповідно до стандартів СОУ Н НБУ 65.1 СУІБ 1.0:2010, СОУ Н НБУ 65.1 СУІБ 2.0:2010, методів двофакторної автентифікації, дослідження відповідних атак на системи банківських транзакцій та вивчення методів протидії;

дослідження формування цифрового підпису за допомогою протоколів інфраструктури відкритих ключів (ІВК).

Навчальна дисципліна "Захист інформації" розглядає принципи побудови комплексних систем і механізми захисту інформації, що засновані на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем. Ці процеси забезпечують надання основних послуг безпеки в інформаційних системах і комп'ютерних мережах (ІСтаКМ), закладають основні принципи цифрової стеганографії й особливості використання центрів сертифікації ключів на основі інфраструктури відкритих ключів (ІВК).

Об'єктом є процес вивчення основних положень теорії захисту інформації, міжнародних і національних стандартів з питань організації безпеки, методів і процедур забезпечення основних послуг з безпеки.

Предметом вивчення дисципліни є методи та процедури забезпечення основних послуг з безпеки відповідно до вимог міжнародних і національних стандартів у галузі захисту інформації.

Необхідна навчальна база перед початком вивчення дисципліни: з метою кращого засвоєння навчального матеріалу дисципліни студенти мають до його початку опанувати знання та навички в галузі дискретної математики, комп'ютерної техніки та комп'ютерних мереж і фахових навчальних дисциплін – "Програмування", "Комп'ютерні мережі". У свою чергу, знання з цієї навчальної дисципліни забезпечують успішне виконання курсових і дипломних проектів.

У процесі навчання студенти здобувають необхідні знання під час лекційних занять і виконання лабораторних завдань. Велике значення в процесі вивчення та закріплення знань має самостійна робота студентів.

У результаті вивчення навчальної дисципліни студент повинен:

знати:

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

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

механізми та протоколи забезпечення конфіденційності даних;

механізми та протоколи забезпечення автентичності (доступності) інформації в банківських системах;

механізми та протоколи забезпечення цілісності даних;

моделі порушника, основні види атак, принципи лінійного та диференційного криптоаналізу;

механізми та протоколи управління ключами в ІВК інформаційної системи;

методи та процедури захисту в банківських системах;

уміти:

визначати вимоги політики безпеки та формувати профіль захисту відповідно до забезпечення послуг з безпеки;

ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів і протоколів захисту інформації;

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

аналізувати технічні параметри чинних протоколів і механізмів захисту інформації з точки зору використання в комп'ютерних системах і мережах, впливу їх характеристик на основні показники комунікаційних систем у цілому;

проводити аналіз ефективності прийнятих технічних рішень щодо забезпечення захисту інформації в банківських системах, користуватися математичним і статистичним апаратом щодо дослідження статистичної крипостійкості механізмів;

забезпечувати захист програмного й інформаційного забезпечення від несанкціонованих дій;

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

У процесі викладання навчальної дисципліни основна увага приділяється оволодінню студентами професійними компетентностями відповідно до Національної рамки кваліфікацій України, яка наведена в додатку А.

3. Програма навчальної дисципліни

Змістовий модуль 1. Безпека та 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 і системах. Вимоги щодо безпеки системи, риски безпеки. Послуги з безпеки: конфіденційність, цілісність, доступність, причетність, спостережність. Розподіл послуг безпеки за рівнями моделі *ISO/OSI*. Критерії захищеності комп'ютерних систем. Розроблення профілю захисту. Механізми реалізації послуг з безпеки. Стандарт *ISO*-7498-2. Побудування та впровадження систем захисту інформації.

Тема 2. Механізми та політики розмежування прав доступу

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

Тема 3. Методи та пристрої забезпечення захисту та безпеки

Компоненти криптосистеми й їх функціональні характеристики. Побудова класифікацій криптографічних засобів. Захист інформації за допомогою міжмережевих екранів.

Тема 4. Захист, доступ та автентифікація

Загальні механізми забезпечення безпеки. Взаємозв'язок послуг і механізмів безпеки, 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 у процесі управління, у тому числі з привілеями. Моделі безпеки. які застосовують для побудови захисту в СУБД. Захист БД у системах з видаленим доступом. Інтерфейси *CGI*, *API* та *FastCGI*.

Тема 6. Шифрування даних

Математичні основи сучасної теорії захисту інформації. Методи булевої алгебри, елементи кореляційного та спектрального аналізів. Прості шифри. Симетричне шифрування даних. Криптографічні примітиви та типи структур симетричного шифрування. Блочні симетричні шифри, алгоритми блокового симетричного шифрування *DES*, ГОСТ-28147, Rijndael, Калина-256. Архітектура блочних симетричних шифрів. Типові режими роботи криптосистеми: "Електронна кодова книга", "Зчеплення блоків шифру", "Зворотний зв'язок з шифру", "Зворотний зв'язок з виходу". Потокові шифри. Регістри зсуву зі зворотнім зв'язком. Асиметричне шифрування даних. Математичні положення теорії скінченних полів і систем класів лишків. Математичні положення теорії чисел. Асиметричні алгоритми шифрування даних *RSA* й Ель Гамаля.

Тема 7. Управління відновленням

Захист і відновлення даних. Формування служб резервного копіювання та відновлення даних для критично-важливих серверів. Кластеризація 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-числові задачі, складність арифметики точок ЕК у різних формах і поданні. Цифрова стеганографія з відкритим ключем.

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

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

Змістовий 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 і 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 із секретним ключем

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

Тема 12. Алгоритми з відкритим ключем

Системи захисту *PGP* і *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 під час підключення до мережі Інтернет. Використання паролів і механізмів контролю.

4. Структура навчальної дисципліни

Із самого початку вивчення навчальної дисципліни кожен студент має бути ознайомлений як з робочою програмою навчальної дисципліни і формами організації навчання, так і зі структурою, змістовністю й обсягом кожного з її навчальних модулів, а також з усіма видами контролю та методикою оцінювання сформованих професійних компетентностей.

Вивчення студентом навчальної дисципліни відбувається шляхом послідовного та ґрунтовного опрацювання навчальних модулів. Навчальний модуль – це окремий, відносно самостійний блок дисципліни, який логічно об'єднує кілька навчальних елементів за змістовністю та взаємозв'язками. Тематичний план дисципліни складається з двох змістових модулів (табл. 4.1).

Таблиця 4.1

Структура залікового кредиту навчальної дисципліни

Теми	Кількість годин									
	денна форма					заочна форма				
	усього	лекції	лабораторні заняття	підсумковий контроль	самостійна робота	усього	лекції	лабораторні заняття	підсумковий контроль	самостійна робота
1	2	3	4	5	6	7	8	9	10	11
Змістовий модуль 1. Безпека та захист даних										
Тема 1. Огляд безпеки системи	3	1	–	–	2	3	1	1	–	4
Тема 2. Механізми та політики розмежування прав доступу	5	1	–	–	4	5	1	1	–	4
Тема 3. Методи та пристрої забезпечення захисту та безпеки	3	1	–	–	2	3	1	1	–	4

Закінчення табл. 4.1

1	2	3	4	5	6	7	8	9	10	11
Тема 4. Захист, доступ та автентифікація	7	1	4	–	2	7	1	1	–	4
Тема 5. Моделі захисту. Захист пам'яті	3	1	–	–	2	3	1	1	–	4
Тема 6. Шифрування даних	13	1	8	–	4	13	1	1	–	4
Тема 7. Управління відновленням	3	1	–	–	2	3	1	1	–	4
Тема 8. Основні напрями розвитку сучасної криптографії	13	1	4	–	8	13	1	1	–	6
Тема 9. Механізми та протоколи управління ключами в ІВК інформаційної системи	16	2	8	–	6	16	2	1	–	4
Разом за змістовим модулем 1	**66**	**10**	**24**	**–**	**32**	**66**	**10**	**9**	**–**	**38**
Змістовий модуль 2. Мережева безпека										
Тема 10. Основні види атак, принципи криптоаналізу. Основи криптографії	12	2	4	–	6	12	2	1	–	7
Тема 11. Алгоритми із секретним ключем	10	2	4	–	4	10	2	1	–	7
Тема 12. Алгоритми з відкритим ключем	12	2	4	–	6	12	2	1	–	7
Тема 13. Протоколи автентифікації	5	1	–	–	4	5	1	1	–	7
Тема 14. Цифрові підписи	9	1	4	–	4	9	1	1	–	7
Тема 15. Використання паролів і механізмів контролю за доступом	4	2	–	–	2	4	2	2	–	9
Разом за змістовим модулем 2	**52**	**10**	**16**	**–**	**26**	**52**	**10**	**7**	**–**	**44**
Залік	2	–	–	2	–	2	–	–	2	–
Усього годин	**120**	**20**	**40**	**2**	**58**	**120**	**20**	**16**	**2**	**82**

5. Теми лабораторних занять

Лабораторне заняття – форма навчального заняття, за якої студент під керівництвом викладача особисто проводить імітаційні експерименти чи досліди з метою практичного підтвердження окремих теоретичних положень навчальної дисципліни. У ході лабораторних робот студент набуває професійних компетенцій та практичних навичок роботи з комп'ютерним обладнанням і відповідними програмними продуктами. За результатами виконання завдання на лабораторному занятті студенти оформлюють індивідуальні звіти з його виконання та захищають їх перед викладачем (табл. 51).

Таблиця 5.1

Теми лабораторних занять

№ п/п	Назви лабораторних робіт	Кількість годин	Рекомендована література
1	Класичні симетричні системи. Дослідження крипостійкості простих симетричних шифрів	4	Основна: [1 – 4]
2	Дослідження сучасних блочних симетричних шифрів і режимів шифрування	4	Основна: [1 – 4]. Додаткова: [5 – 9]
3	Дослідження сучасних асиметричних крипто-систем шифрування. Стандарт ДСТУ *ISO\IEC* 15948-2	4	Основна: [1 – 4]. Додаткова: [5 – 9]
4	Дослідження електронного цифрового підпису. ЦП Ель Гамаля, ДСТУ-4145, *ECDSA*	4	Основна: [1 – 4]. Додаткова: [5 – 9]
5	Стеганографічні методи захисту інформації	4	Основна: [1 – 4]. Додаткова: [5 – 9]
6	Безпечність персональних конфіденційних даних на базі секретного диску та захищеної електронної пошти *PGP*	4	Основна: [1 – 4]. Додаткова: [5 – 9]
7	Статистичні дослідження генераторів випадкових і псевдовипадкових послідовностей за мето-дикою *NIST*	4	Основна: [1 – 4]. Додаткова: [5 – 9]
8	Розгортання й управління інфраструктурою відкритих ключів	12	Основна: [1 – 4]. Додаткова: [5 – 9]
Усього		**40**	

У ході виконання лабораторних робіт 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 та використання відповідних програмних засобів і додатків.

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

5.1. Приклади типових лабораторних завдань за темами

Змістовий модуль 1. Безпека та захист даних

Тема 6. Шифрування даних

1. Виконати реалізацію простих шифрів – зашифрувати своє прізвище та повне ім'я.

2. Провести статистичний криптоаналіз.

3. Підготувати звіт встановленого зразка, в якому розписати порядок шифрування кожним з розглянутих простих шифрів, надати результати криптоаналізу.

Змістовий модуль 2. Мережева безпека

Тема 3. Методи та пристрої забезпечення захисту та безпеки

1. Повторити призначення й основні можливості програми Pretty Good Privacy (*PGP*) щодо забезпечення безпеки електронної пошти.

2. Усвідомити порядок застосування відкритого й особистого ключів для захисту електронного листування та гарантії достовірності джерела повідомлення.

2.1. Згенерувати пару ключів: відкритий і особистий.

2.2. Скласти, зашифрувати й обмінятися шифрованими електронними повідомленнями; розшифрувати прийняті повідомлення.

2.3. Скласти, підписати й обмінятися електронними повідомленнями; перевірити достовірність джерел повідомлень.

2.4. Скласти, підписати, зашифрувати й обмінятися електронними повідомленнями; розшифрувати прийняті повідомлення і перевірити достовірність джерел повідомлень.

6. Самостійна робота студента

Самостійна робота студента (СРС) – це форма організації навчального процесу, за якої заплановані завдання виконує студент самостійно під методичним керівництвом викладача.

Мета СРС – засвоєння в повному обсязі навчальної програми та формування у студентів загальних і професійних компетентностей, які відіграють суттєву роль у становленні майбутнього фахівця вищого рівня кваліфікації.

Навчальний час, відведений для самостійної роботи студентів денної форми навчання, визначається навчальним планом і становить 50 % (60 години) від загального обсягу навчального часу на вивчення дисципліни (120 годин). У ході самостійної роботи студент має перетворитися на активного учасника навчального процесу, навчитися свідомо ставитися до оволодіння теоретичними знаннями та практичними навичками, вільно орієнтуватися в інформаційному просторі, нести індивідуальну відповідальність за якість власної професійної підготовки. СРС включає: опрацювання лекційного матеріалу; опрацювання та вивчення рекомендованої літератури, основних термінів і понять за темами дисципліни; підготовку до лабораторних занять; поглиблене опрацювання окремих лекційних тем або питань; пошук (підбір) та огляд літературних джерел за заданою проблематикою дисципліни; аналітичний розгляд наукових публікацій; перевірку власних знань за контрольними запитаннями; підготовку до контрольних робіт та інших форм поточного контролю; систематизацію вивченого матеріалу з метою підготовки до семестрового екзамену. Основні види самостійної роботи, які запропоновані студентам для засвоєння теоретичних знань з навчальної дисципліни, наведені в табл. 6.1.

Таблиця 6.1

Завдання для самостійної роботи студентів і форми її контролю

Теми	Змістовність самостійної роботи студентів	Кількість годин	Форми контролю СРС	Рекомендована література
1	2	3	4	5
Змістовий модуль 1. Безпека та захист даних				
Тема 1. Огляд безпеки системи	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Життєвий цикл політики безпеки. 2. Принципи побудови системи захисту інформації. 3. Проект профілю безпеки	2	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]

Продовження табл. 6.1

1	2	3	4	5
Тема 2. Механізми та політики розмежування прав доступу	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Безпека доступу до коду в **.NET*. 2. Розмежування доступу процесів до системного диска в ОС Windows 7/ Server 2008 R2. 3. Розмежування доступу процесів до системного диска в ОС Unix і Linux	4	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]
Тема 3. Методи та пристрої забезпечення захисту та безпеки	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Генератори випадкових чисел. 2. Біометричні пристрої автентифікації. 3. Криптопровайдери. 4. Мережеві політики фільтрації трафіку	2	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]
Тема 4. Захист, доступ та автентифікація	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Цілісність з'єднання з відновленням. 2. Обмін аутентичними ключами за допомогою асиметричної криптосистем. 3. Протоколи автентифікації для забезпечення безпеки в мережі Internet	2	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]

Продовження табл. 6.1

1	2	3	4	5
Тема 5. Моделі захисту. Захист пам'яті	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Використання BitLocker для захисту персональних даних в *OS Windows* 7, 10. 2. Використання *PGP* Disk для захисту персональних даних	2	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]
Тема 6. Шифрування даних	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Шифрування конфіденційної інформації на флешносіях. 2. Шифрування даних в сучасних протоколах передання інформації. 3. Алгоритм Advanced Encryption Standard (*AES*, алгоритм Rijndael)	4	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]
Тема 7. Управління відновленням	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Повне видалення даних з носіїв інформації. 2. Механізми відновлення паролів в ОС. 3. Системи резервного копіювання дисків	2	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]
Тема 8. Основні напрями розвитку сучасної криптографії	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Огляд стеганоалгоритмів, що дозволяють вбудовувати інформацію у зображення. 2. Криптоаналіз на основі квантової криптографії	8	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]

Продовження табл. 6.1

1	2	3	4	5
Тема 9. Механізми та протоколи управління ключами в ІВК інформаційної системи	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Проблеми та ризики технології ІВК. 2. Розгортання інфраструктури відкритих ключів. 3. Програмні засоби підтримки PKI	6	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]
Усього за змістовим модулем 1		**32**		
Змістовий модуль 2. Мережева безпека				
Тема 10. Основні види атак, принципи криптоаналізу. Основи криптографії	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Факторизація. Метод факторизації загальне решето числового поля. 2. Методи розв'язання дискретного логарифму в групі точок еліптичної кривої. 3. Загрози та атаки проникнення в інформаційну систему	6	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]
Тема 11. Алгоритми із секретним ключем	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Шифрування трафіку в протоколі *IPSec*. 2. Шифрування трафіку та забезпечення цілісності даних у протоколі *SSL*. 3. Шифрування трафіку та забезпечення цілісності даних у протоколі *TLS*	4	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]

Закінчення табл. 6.1

1	2	3	4	5
Тема 12. Алгоритми з відкритим ключем	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Модель використання відкритих ключів у системі *PGP*	6	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]
Тема 13. Протоколи автентифікації	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Прості функції гешування. Захист функцій гешування. 2. Методи автентифікації віддаленого користувача в мережі Internet. 3. Протокол видаленої реєстрації *SHH*	4	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]
Тема 14. Цифрові підписи	Вивчення лекційного матеріалу, підготовка до лабораторного заняття. *Самостійне опрацювання лекційного матеріалу*: 1. Сліпий цифровий підпис. 2. Разовий цифровий підпис. 3. Стандарти цифрового підпису на еліптичній кривій	4	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]
Тема 15. Використання паролів і механізмів контролю за доступом	Вивчення лекційного матеріалу, підготовка до лабораторного заняття	2	Експрес-опитування	Основна: [1 – 4]. Додаткова: [5 – 9]
Усього за змістовим модулем 2		**26**		
Залік		2		
Усього		**60**		

6.1. Тематика контрольних робіт для студентів заочної форми навчання

Контрольна робота є однією з форм контролю й обліку знань та умінь студентів. Розрізняють контрольні роботи, які виконують за семестровим розкладом занять, на заліках та екзаменах. Особливе місце належить контрольним роботам, які виконані студентами заочного навчання. Контрольна робота, будучи засобом контролю, виконує навчальні та виховні функції. Контрольні роботи проводяться, як правило, у письмовій формі.

Контрольні роботи, виконувані *за семестровим розкладом занять*, проводяться за дисциплінами згідно з навчальними планами та робочими навчальними програмами за рахунок часу, відведеного на вивчення дисципліни. Їх змістовність може охоплювати найбільш важливі розділи (теми) навчальних дисциплін або весь навчальний матеріал, вивчений до її проведення. Студенти заочної форми навчання виконують контрольні роботи, як правило, в обсязі робочих навчальних програм дисциплін.

Змістовність 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, творчої активності, узагальнень, установлення зв'язку теорії з практикою. Завдання, як правило, містять теоретичні та практичні питання, мають 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, враховувати рівень підготовки студентів. За такого варіювання завдань контрольна робота дає найбільш повне й об'єктивне уявлення про знання й уміння студентів навчальної групи.

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

Лектор потоку у вступній лекції з 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 до відома студентів оцінок за нею повинні здійснюватися у мінімальні строки. Чим більше відстрочений за часом аналіз результатів контрольної роботи, тим нижча 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. Вона включає п'ять практичних завдань, які потрібно пов'язати із практикою відпрацювання на мережі шляхом її адміністрування.

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

Варіанти задач до контрольних робіт

Завдання 1. Виконати шифрування та розшифрування свого прізвища, імені та по батькові за всіма методами шифрування (табл. 6.2).

Провести оцінювання криптографічної стійкості шифрів на основі порівняння множини ключів (кількості) K і множини отримуваних криптограм C. Завдання виконати відповідно до варіанта (див. табл. 6.2).

Порівняти статистичну залежність криптограм і відкритого тексту.

Таблиця 6.2

Варіанти завдання

№ варіанта	Методи шифрування
1	Шифр Плейфера. Поліалфавітна заміна
2	Перестановочний шифр із ключовим словом. Шифр "Квадрат Цезаря"
3	Шифр простої заміни. Шифр із автоключем з використанням відкритого тексту
4	Афінна криптосистема. Поліалфавітна заміна
5	Шифр Цезаря. Шифр Віженера
6	Шифр Цезаря із ключовим словом. Шифр простої заміни
7	Матрична перестановка. Поліалфавітна заміна
8	Шифр Плейфера. 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 шістьма користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (розшифрування) *RSA* та створювати або перевіряти цифровий підпис на основі *RSA* для повідомлень.

Таблиця 6.3

Користувачі системи

Користувачі	Параметри 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".

Перевірте, чи ваші ключі (відкритий і особливий) відібрані правильно.

Розшифруйте повідомлення M, отримано від користувача "F".

Таблиця 6.4

Формат повідомлення

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

Завдання 3. Виконати аналіз загроз безпеки підприємства, на якому працює студент. Розробити політику безпеки підприємства зазначивши типи конфіденційної інформації, методи криптографічного методи мережевого захисту.

6.2. Контрольні запитання для самоперевірки

Тема 1. Огляд безпеки системи

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

Тема 2. Механізми та політики розмежування прав доступу

1. Загрози подолання розмежувальної 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.
7. Правила призначення міток безпеки ієрархічним об'єктам доступу.
8. Безпека доступу до коду в *.NET*.
9. Розмежування доступу процесів до системного диска в ОС Windows 7/ Server 2008 R2.
10. Розмежування доступу процесів до системного диска в ОС Unix і Linux.

Тема 3. Методи та пристрої забезпечення захисту та безпеки

1. Генератори випадкових чисел.
2. Біометричні пристрої автентифікації.
3. Криптопровайдери.

4. Мережеві політики фільтрації трафіку.

5. Особливості міжмережевого екранування на різних рівнях моделі *OSI*.

6. Архітектура сучасного міжмережевого екрану.

Тема 4. Захист, доступ та автентифікація

1. Автентифікація джерела даних та об'єкта комунікацій.

2. Конфіденційність з'єднання, трафіку, віддаленого поля даних.

3. Цілісність з'єднання з відновленням.

4. Обмін автентичними ключами за допомогою асиметричної криптографії.

5. Протоколи доступа для забезпечення безпеки в мережі Internet.

6. Реалізація системи автентифікації на основі служби каталогів.

7. Реалізація системи автентифікації відкритих ключів без підтримки служби каталогів.

Тема 5. Моделі захисту. Захист пам'яті

1. Розподіл пам'яті в операційних системах.

2. Прозоре шифрування даних.

3. Механізми захисту ключів.

4. Мандатна адресація.

5. Використання BitLocker для захисту персональних даних в OS Windows 7, 10.

6. Використання PGP Disk для захисту персональних даних.

Тема 6. Шифрування даних

1. Механізми забезпечення конфіденційності 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. Алгоритм Каліна–256.
9. Схеми спрямованого шифрування на еліптичній кривій.
10. Шифрування конфіденційної інформації на флеш-носіях.
11. Шифрування даних в сучасних протоколах передавання інформації.

Тема 7. Управління відновленням

1. Повне видалення даних з носіїв інформації.
2. Механізми відновлення паролів в ОС.
3. Системи резервного копіювання дисків.
4. Журналізація змін.
5. План резервного відновлення БД після збою.
6. Методи відновлення БД після помилки в обробці даних.

Тема 8. Основні напрями розвитку сучасної криптографії

1. Теорія чисел і криптографія.
2. Атаки на стеганографічні системи.
3. Зниження обчислювальної складності криптографічних перетворень.
4. Квантова криптографія.
5. Колективні криптографічні протоколи.
6. Огляд стеганоалгоритмів, що дозволяють вбудовувати інформацію у зображення.
7. Криптоаналіз на основі квантової криптографії.

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

1. Політика використання сертифікатів.
2. Сертифікати відкритих ключів X.509.
3. Компоненти та сервіси інфраструктури відкритих ключів.
4. Списки скасованих сертифікатів.
5. Політика ІВК.
6. Проблеми та ризики технології ІВК.
7. Розгортання інфраструктури відкритих ключів.
8. Програмні засоби підтримки PKI.

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

1. Модель порушника.
2. Вимоги до сучасних криптоалгоритмів.
3. Факторизація. Метод факторизації "загальне решето числового поля".
4. Методи розв'язання дискретного логарифму в групі точок еліптичної кривої.
5. Загрози й атаки проникнення в інформаційну систему.
6. Параметри криптоалгоритмів і складність криптоатак.

Тема 11. Алгоритми із секретним ключем

1. Побудування *VPN*-мереж.
2. Ключові та безключові геш-функції.
3. Шифрування трафіку в протоколі *IPSec*.
4. Шифрування трафіку та забезпечення цілісності даних в протоколі *SSL*.
5. Шифрування трафіку та забезпечення цілісності даних в протоколі *TLS*.
6. Захищеність VPN-мереж.
7. Механізми забезпечення конфіденційності даних на прикладному рівні моделі OSI.

Тема 12. Алгоритми з відкритим ключем

1. Управління 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*.
5. Використання протоколу узгодження ключів в протоколах *SSL* і *TLS*.
6. Перевага асиметричної криптографії над симетричною.

Тема 13. Протоколи автентифікації

1. Механізми забезпечення автентичності на основі сучасних асиметричних процедур шифрування, *MAC*-кодів.
2. Сучасні алгоритми гешування.

3. Автентифікація повідомлень і геш-функція гешування.

4. Прості функції гешування. Захист функцій гешування.

5. Методи автентифікації віддаленого користувача в мережі Internet.

6. Протокол видаленої реєстрації SHH.

Тема 14. Цифрові підписи

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.

6. Юридичні аспекти використання цифрового підпису в Україні.

7. Європейські стандарти цифрового підпису, що гармонізовані в Україні.

Тема 15. Використання паролів і механізмів контролю за доступом

1. Протокол Нідхема і його реалізація в операційній системі *UMIX*.

2. Схема з одноразовими паролями.

3. Механізми реалізації дискреційної моделі доступу.

4. Механізми реалізації мандатної моделі доступу.

5. Реалізація пріоритетних розкладів в сучасних ОС.

6. Контроль за діями користувачів в ОС Windows 7/Server 2008.

7. Індивідуально-консультативна робота

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.

8. Методи навчання

У процесі викладання навчальної дисципліни для активізації навчально-пізнавальної діяльності студентів передбачене застосування як активних, так і інтерактивних навчальних технологій, серед яких: лекції проблемного характеру, міні-лекції, робота в малих групах, семінари-дискусії, мозкові атаки, кейс-метод, презентації, ознайомлювальні (початкові) ігри, метод проектної роботи, комп'ютерні симуляції, метод Дельфі, метод сценаріїв, банки візуального супроводу (табл. 8.1).

Таблиця 8.1

Розподіл форм та методів активізації процесу навчання за темами навчальної дисципліни

Теми	Практичне застосування навчальних технологій
1	2
Тема 1. Огляд безпеки системи	*Проблемна лекція* "Визначення базових засад захисту інформації в інформаційній системі підприємства"
Тема 2. Механізми та політики розмежування прав доступу	*Проблемна лекція* "Визначення базових засад захисту інформації в інформаційній системі підприємства"
Тема 3. Методи та пристрої забезпечення захисту та безпеки	*Міні-лекції* "Використання сучасних методів шифрування в протоколах мережі Internet"
Тема 4. Захист, доступ та автентифікація	*Метод сценаріїв* "Визначення ймовірних моделей поведінки та розвитку правопорушника або інсайдера"

Закінчення табл. 8.1

1	2
Тема 5. Моделі захисту. Захист пам'яті	*Міні-лекції* "Використання сучасних методів шифрування в хмарних сховищах даних"
Тема 6. Шифрування даних	*Мозгова атака* "Визначення крипостійкості блоково-симетричних шифрів"
Тема 7. Управління відновленням	*Лекція проблемного характеру* "Можливості адміністрування в сучасних корпоративних мережах"
Тема 8. Основні напрями розвитку сучасної криптографії	*Лекція проблемного характеру* "Можливості методів цифрової стеганографії зі забезпечення прихованості передавання даних в мережі Internet"
Тема 9. Механізми та протоколи управління ключами в ІВК інформаційної системи	*Банк візуального супроводження* "Механізми використання цифрових сертифікатів"
Тема 10. Основні види атак, принципи криптоаналізу. Основи криптографії	*Метод сценаріїв* "Визначення ймовірних моделей поведінки та розвитку правопорушника або інсайдера", *Метод Дельфі* "Статистична оцінка крипостійкості за допомогою пакета *NIST STS*"
Тема 11. Алгоритми із секретним ключем	*Лекція проблемного характеру* "Можливості криптосистем щодо забезпечення конфіденційності передавання даних в мережі Internet"
Тема 12. Алгоритми з відкритим ключем	*Проблемна лекція* "Визначення засобів захисту від НСД в інформаційній системі підприємства. Розгортання інфраструктури відкритих ключів". *Ділова гра* "Обґрунтування вибору механізмів захисту для забезпечення ефективного використання інформації на підприємстві"
Тема 13. Протоколи автентифікації	*Лекція проблемного характеру* "Можливості використання методів двофакторної автентифікації"
Тема 14. Цифрові підписи	*Лекція проблемного характеру* "Можливості використання методів двофакторної автентифікації"
Тема 15. Використання паролів і механізмів контролю за доступом	*Лекція проблемного характеру* "Можливості адміністрування в сучасних корпоративних мережах"

Основні відмінності активних та інтерактивних методів навчання від традиційних визначаються не тільки методикою та технікою викладання, але й високою ефективністю навчального процесу, що проявляється у: високій мотивації студентів; практичному закріпленні теоретичних знань; підвищенні самосвідомості студентів; формуванні здатності до прийняття самостійних і до ухвалення колективних рішень; формуванні здатності до соціальної інтеграції; набуття навичок вирішення конфліктів; розвитку здатності до знаходження компромісів.

Лекції проблемного характеру – один із найважливіших елементів проблемного навчання студентів. Вони передбачають, поряд із розглядом основного лекційного матеріалу, визначення та розгляд кола проблемних питань дискусійного характеру, які недостатньо розроблені в науці та мають актуальні для теорії та практики. Лекції проблемного характеру відрізняються поглибленою аргументацією матеріалу, що викладається. Вони сприяють формуванню у студентів самостійного творчого мислення, прищеплюють їм пізнавальні навички. Студенти стають учасниками наукового пошуку та вирішення проблемних ситуацій.

Міні-лекції передбачають викладення навчального матеріалу за короткий проміжок часу та характеризуються значною ємністю, складністю логічних побудов, образів, доказів та узагальнень. Вони проводяться, як правило, як частина заняття-дослідження. Міні-лекції відрізняються від повноформатних лекцій значно меншою тривалістю. Зазвичай міні-лекції тривають не більше 10 – 15 хвилин і використовуються для того, щоб стисло донести нову інформацію до всіх студентів. Міні-лекції часто застосовуються як частини цілісної теми, яку бажано викладати повноформатною лекцією, щоб не втомлювати аудиторію. Тоді інформація надається послідовно кількома окремими сегментами, між якими застосовуються інші форми та методи навчання.

Семінари-дискусії передбачають обмін думками та поглядами учасників з приводу даної теми, а також розвивають мислення, допомагають формувати погляди та переконання, виробляють уміння формулювати думки та висловлювати їх.

Робота в малих групах дає змогу структурувати практично-семінарські заняття за формою та змістовністю, створює можливості для участі кожного студента в роботі за темою заняття, забезпечує формування особистісних якостей та досвіду соціального спілкування.

Мозкові атаки – метод розв'язання невідкладних завдань, сутність якого полягає в тому, щоб висловити якомога більшу кількість ідей за дуже обмежений проміжок часу, обговорити та здійснити їх селекцію.

Презентації – виступи перед аудиторією, що використовуються для представлення певних досягнень, результатів роботи групи, звіту з виконання індивідуальних завдань, проектних робіт. Презентації можуть бути як індивідуальними (наприклад, виступ одного студента), так і колективними, тобто виступи двох та більше студентів.

Метод Дельфі використовується з метою досягнення консенсусу в експертних оцінках і передбачає надання можливості висловити свої думки групі експертів, які працюють індивідуально в різних місцях. Для вибору управлінського рішення за цим методом академічну групу розділяють, наприклад, на п'ять малих груп. Чотири групи є робочими, вони розробляють і приймають управлінське рішення, а п'ята група є експертною. Аналіз і варіанти управлінських рішень робочих груп усереднюються цією групою. Експертна група може бути розподілена за спеціалізацією.

Комп'ютерна симуляція (гра) – це метод навчання, що спирається на використання спеціальних комп'ютерних програм, за допомогою яких можливе віртуальне моделювання бізнес-процесу. Студенти можуть змінювати параметри та дані, приймати рішення й аналізувати їх наслідки. Метою використання даного методу є розвиток системного мислення студентів, їх здібностей до планування, формування вмінь розпізнавати й аналізувати проблеми, порівнювати й оцінювати альтернативи, приймати оптимальні рішення та діяти в умовах обмеженого часу.

Метод сценаріїв полягає в розробленні ймовірних моделей поведінки та розвитку конкретних явищ у перспективі.

Банки візуального супроводу сприяють активізації процесу навчання за темами навчальної дисципліни за допомогою наочності.

9. Методи контролю

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних, практичних, семінарських занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

модульний контроль, що проводиться з урахуванням поточного контролю за відповідний змістовий модуль і має на меті *інтегровану* оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

Поточний контроль з даної навчальної дисципліни проводиться в таких формах:

активна робота на лекційних заняттях;

активна участь у виконанні лабораторних завдань;

проведення письмової контрольної роботи;

експрес-опитування.

Модульний контроль з даної навчальної дисципліни проводиться у формі письмової контрольної роботи.

Підсумковий/семестровий контроль проводиться у формі семестрового екзамену. ***Семестрові екзамени*** – форма оцінювання підсумкового засвоєння студентами теоретичного та практичного матеріалу з окремої навчальної дисципліни, що проводиться як контрольний захід.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час лабораторних занять проводиться 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;

уміння поєднувати теорію з практикою під час розгляду виробничих ситуацій, розв'язання задач, проведення розрахунків у процесі виконання індивідуальних завдань під час лабораторних занять;

логіка, структура, стиль подання матеріалу в письмових роботах, уміння обґрунтовувати свою позицію, здійснювати узагальнення інформації та робити висновки.

Максимально можливий бал за конкретним завданням ставиться за умови відповідності індивідуального завдання студента або його усної відповіді всім зазначеним критеріям. Відсутність тієї або іншої складової знижує кількість балів. В оцінюванні індивідуальних завдань увага також приділяється якості, самостійності та своєчасності надання виконаних завдань викладачу, згідно з графіком навчального процесу. Якщо якась із вимог не буде виконана, то бали будуть знижені.

Поточна контрольна робота проводиться два рази за семестр і включає практичні завдання різного рівня складності відповідно до тем змістового модуля.

Критерії оцінювання позааудиторної самостійної роботи студентів. Загальними критеріями, за якими здійснюється оцінювання позааудиторної самостійної роботи студентів, є: глибина та міцність знань; рівень мислення; вміння систематизувати знання за окремими темами та робити обґрунтовані висновки; володіння категорійним апаратом; навички та прийоми виконання практичних завдань; уміння знаходити необхідну інформацію, здійснювати її систематизацію й обробку; самореалізація на лабораторних заняттях.

Порядок підсумкового контролю з навчальної дисципліни. Підсумковий контроль знань і компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену. Екзаменаційний білет охоплює програму дисципліни та передбачає визначення рівня знань і ступеня опанування студентами компетентностей. Зразок екзаменаційного білета наведений у додатку Б.

Завданням екзамену є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності до творчого використання накопичених знань, уміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо. В умовах реалізації компетентнісного підходу екзаменатор оцінює рівень засвоєння студентом компетентностей, що передбачені кваліфікаційними вимогами. Кожен екзаменаційний білет складається із трьох практичних завдань, які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента та рівень його компетентності з навчальної дисципліни, які оцінюються відповідно до Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця.

Студент, який із поважних причин, підтверджених документально, не мав можливості брати участь у формах поточного контролю (тобто не склав змістовий модуль), за розпорядженням декана факультету відповідно до встановленого терміну має право на його відпрацювання у двотижневий термін після повернення до навчання.

Студент **не може бути допущений** до складання екзамену, якщо кількість балів, отриманих за результатами перевірки успішності під час поточного та модульного контролю відповідно до змістового модуля

впродовж семестру, в сумі не досягла 35 балів. Після екзаменаційної сесії декан факультету видає розпорядження про ліквідацію академічної заборгованості. У встановлений термін студент добирає залікові бали.

Студента слід **вважати атестованим**, якщо сума балів, отриманих за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 і мінімально можлива кількість балів, набраних на екзамені, – 25.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі *екзаменаційної "Відомості обліку успішності"*.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: *"60 і більше балів – зараховано", "59 і менше балів – не зараховано"* – та заноситься у *залікову "Відомість обліку успішності"* навчальної дисципліни. У випадку отримання менше 60 балів студент обов'язково здає залік після закінчення екзаменаційної сесії у встановлений деканом факультету термін, але не пізніше двох тижнів після початку семестру. У випадку повторного отримання менше 60 балів декан факультету призначає комісію у складі трьох викладачів на чолі із завідувачем кафедри та визначає термін перескладання заліку, після чого приймається рішення відповідно до чинного законодавства: "зараховано" – студент продовжує навчання за графіком навчального процесу; а якщо "не зараховано", тоді декан факультету пропонує студенту повторне вивчення навчальної дисципліни протягом наступного навчального періоду самостійно.

Підсумкові бали за екзамен складаються із суми балів за виконання всіх завдань, що округлені до цілого числа за правилами математики.

Кожне з практичних завдань і теоретичне питання оцінюється за 10-бальною системою з наступною підсумковою оцінкою за виконання всього екзаменаційного завдання. Загальна сума – 40 балів.

Передбачається використовувати такі критерії для виставлення оцінок.

Завдання 1.

Теоретичні питання (10 запитань) з основних положень дисципліни. Кожне питання оцінюється в 1 бал.

Завдання 2.

Оцінка 10 балів. Практичне завдання виконане бездоганно з повним обґрунтуванням кожного етапу виконання, зроблені повні висновки й узагальнення. Наведені алгоритми шифрування/розшифрування з поясненнями, сформована криптограма відповідає алгоритму шифрування, стійкість алгоритму шифрування оцінена частотним криптоаналізом.

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

Оцінка 8 балів. Практичне завдання виконане повністю. Сформована криптограма відповідає алгоритму шифрування, але не наведені процедури шифрування/розшифрування.

Оцінка 7 балів. Практичне завдання виконано неповністю. Сформована криптограма відповідає алгоритму шифрування, але окремі символи зашифровані неправильно.

Оцінка 6 балів. Практичне завдання виконане неповністю. Сформована криптограма в цілому відповідає алгоритму шифрування, але окремі символи зашифровані неправильно.

Оцінка 5 бали. Практичне завдання виконане неповністю. Сформована криптограма відповідає алгоритму шифрування, але 1/2 символів зашифровані неправильно.

Оцінка 4 бали. Практичне завдання не виконане. Сформована криптограма не відповідає алгоритму шифрування або більше 1/2 символів зашифровані неправильно.

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

Оцінка 2 бали. Практичне завдання не виконане. Сформована криптограма не відповідає алгоритму шифрування або вибраний інший алгоритм шифрування.

Оцінка 1 бал. Практичне завдання не виконане. Не сформована криптограма та вибраний інший алгоритм шифрування.

Оцінка 0 балів. Відповідь на практичне запитання відсутня.

Завдання 3, 4.

Оцінка 10 балів. Практичне завдання виконане бездоганно з повним обґрунтуванням кожного етапу виконання, зроблені повні висновки й узагальнення. Наведений протокол обміну відповідає вимогам відповідного

стандарту, приведені алгоритми шифрування/розшифрування з повними поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), визначені переваги та недоліки обґрунтовані, проведений порівняльний аналіз обґрунтований. Наведені механізми та послуги, в яких використовуються відповідні протоколи (схеми) шифрування.

Оцінка 9 балів. Практичне завдання виконане повністю з обґрунтуванням кожного етапу виконання. Наведений протокол обміну відповідає вимогам відповідного стандарту, приведена структурна схема протоколу з повними поясненнями процедур шифрування/розшифрування, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), визначені основні переваги та недоліки обґрунтовані, в цілому проведений порівняльний аналіз обґрунтований.

Оцінка 8 балів. Практичне завдання виконане повністю. Наведений протокол обміну відповідає вимогам відповідного стандарту, приведені основні процедури шифрування/розшифрування з поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), але не в повному обсязі визначені основні переваги та недоліки, в цілому проведений порівняльний аналіз обґрунтований.

Оцінка 7 балів. Практичне завдання виконане повністю. Наведений протокол обміну відповідає вимогам відповідного стандарту, приведені основні процедури шифрування/розшифрування з поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), але не в повному обсязі визначені переваги та недоліки, проведений порівняльний аналіз не обґрунтований.

Оцінка 6 балів. Практичне завдання виконане повністю. Наведений протокол обміну відповідає вимогам відповідного стандарту, приведені основні процедури шифрування/розшифрування з поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), але не в повному обсязі визначені переваги та недоліки, не проведений порівняльний аналіз.

Оцінка 5 балів. Практичне завдання виконане неповністю. Наведений протокол обміну відповідає вимогам відповідного стандарту, приведені алгоритми шифрування/розшифрування, але сформована криптограма або повідомлення не відповідають алгоритму шифрування/розшифрування, не визначені основні переваги та недоліки, не проведений порівняльний аналіз.

Оцінка 4 бали. Практичне завдання виконане неповністю. Наведений протокол обміну в цілому відповідає вимогам відповідного стандарту, приведені алгоритми шифрування/розшифрування, але сформована криптограма та повідомлення не відповідають алгоритму шифрування/розшифрування, не визначені основні переваги та недоліки, не проведений порівняльний аналіз.

Оцінка 3 бали. Практичне завдання не виконане. Наведений протокол обміну не відповідає вимогам відповідного стандарту, не приведені алгоритми шифрування/розшифрування, сформована криптограма та повідомлення не відповідають алгоритму шифрування/розшифрування, пояснень процедур немає, не визначені переваги та недоліки, не проведений порівняльний аналіз.

Оцінка 2 бали. Практичне завдання не виконане. Протокол обміну не приведений, не приведені алгоритми шифрування/розшифрування, сформована криптограма та повідомлення не відповідають алгоритму шифрування/розшифрування, не визначені переваги та недоліки, не проведений порівняльний аналіз.

Оцінка 1 бал. Практичне завдання не виконане. Не сформована криптограма та вибраний інший протокол механізму безпеки.

Оцінка 0 балів. Відповідь на практичне запитання відсутня.

10. Розподіл балів, які отримують студенти

Система оцінювання рівня сформованості професійних компетентностей студентів денної форми навчання наведена в табл. 10.1.

Таблиця 10.1

Система оцінювання рівня сформованості професійних компетентностей

Професійні компетентності	**Навчальний тиждень**	**Години**		**Форми навчання**		**Оцінка рівня сформованості компетентностей**	
						Форми контролю	**Максимальний бал**
1	2	3		4		5	6
Змістовий модуль 1. Безпека та захист даних							
Здатність визначати основні поняття системи безпеки	**1**	**Аудиторні**	**2**	**Лекція**	*Тема 1.* Огляд безпеки системи	Активна участь на занятті	**1**
			4	**Лабораторне заняття**	*Лабораторна робота 1.* Класичні симетричні системи. Дослідження крипостійкості простих симетричних шифрів	Захист лабораторної роботи	**5**

1	2	3		4		5	6
		СРС	**2**	**Підготовка до занять**	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до лабораторного заняття, експрес-опитування		
Здатність ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів БСШ	**2**	**Аудиторні**	**2**	**Лекція**	*Тема 2.* Механізми та політики розмежування прав доступу. *Тема 3.* Методи та пристрої забезпечення захисту та безпеки	Активна участь на занятті	**1**
			4	**Лабораторне заняття**	*Лабораторна робота 2.* Дослідження сучасних блочних симетричних шифрів та режимів шифрування	Захист лабораторної роботи/ експрес-опитування	**10**
		СРС	**6**	**Підготовка до занять**	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до лабораторного заняття		
Здатність аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів несиметричного шифрування	**3**	**Аудиторні**	**2**	**Лекція**	*Тема 4.* Захист, доступ та автентифікація. *Тема 5*. Моделі захисту. Захист пам'яті	Активна участь на занятті/ поточна КР	**13**
			4	**Лабораторне заняття**	*Лабораторна робота 3.* Дослідження сучасних асиметричних криптосистем шифрування. Стандарт ДСТУ ISO\IEC 15948-2	Захист лабораторної роботи	**5**
		СРС	**4**	**Підготовка до занять**	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до лабораторного заняття, до КР		
Здатність визначати основні поняття ЕЦП. Основні вимоги щодо його формування	**4**	**Аудиторні**	**2**	**Лекція**	*Тема 6.* Шифрування даних. *Тема 7.* Управління відновленням	Активна участь на занятті	**1**
			4	**Лабораторне заняття**	*Лабораторна робота 4*. Дослідження електронного цифрового підпису. ЦП Ель Гамаля, ДСТУ 4145, ECDSA	Захист лабораторної роботи	**5**
		СРС	**6**	**Підготовка до занять**	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до лабораторного заняття, експрес-опитування		
Змістовий модуль 2. Мережева безпека							
Здатність визначати основні поняття сучасних протоколів прихованості інформації на основі цифрової стеганографії	**5**	**Аудиторні**	**2**	**Лекція**	*Тема 8.* Основні напрями розвитку сучасної криптографії	Активна участь на занятті/ поточна КР	**13**
			4	**Лабораторне заняття**	*Лабораторна робота 5.* Стеганографічні методи захисту інформації	Захист лабораторної роботи, експрес-опитування	**9**
		СРС	**8**	**Підготовка до занять**	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до лабораторного заняття		

Закінчення табл. 10.1

1	2	3		4		5	6
Здатність визначати основні алгоритми системи захищеної електронної пошти PGP, функції, механізми	**6**	**Аудиторні**	**2**	**Лекція**	*Тема 11.* Алгоритми із секретним ключем. *Тема 12.* Алгоритми з відкритим ключем	Активна участь на занятті	**1**
			4	**Лабораторне заняття**	*Лабораторна робота 6.* Безпечність персональних конфіденціальних даних на базі секретного диску та захищеної електронної пошти PGP	Захист лабораторної роботи	**5**
		СРС	**10**	**Підготовка до занять**	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до лабораторного заняття, до експрес-опитування, КР		
Здатність визначати основні поняття інфраструктури відкритих ключів	**7**	**Аудиторні**	**2**	**Лекція**	*Тема 9.* Механізми та протоколи управління ключами в ІВК інформаційної системи	Активна участь на занятті	**1**
			4	**Лабораторне заняття**	*Лабораторна робота 7.* Статистичні дослідження генераторів випадкових та псевдовипадкових послідовностей за методикою NIST	Захист лабораторної роботи, експрес-опитування	**10**
		СРС	**6**	**Підготовка до занять**	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до лабораторного заняття		
Здатність визначати основних функцій та протоколів систем PKI, IPSec, SSL (TLS)	**8**	**Аудиторні**	**2**	**Лекція**	*Тема 13.* Протоколи автентифікації. *Тема 14.* Цифрові підписи	Активна участь на занятті, КР	**13**
			4	**Лабораторне заняття**	*Лабораторна робота 8.* Розгортання та управління інфраструктурою відкритих ключів		
		СРС	**8**	**Підготовка до занять**	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до лабораторного заняття		
Здатність виконувати оцінювання криптостійкості на основі методів криптоаналізу	**9**	**Аудиторні**	**2**	**Лекція**	*Тема 10.* Основні види атак, принципи криптоаналізу. Основи криптоаналізу	Активна участь на занятті	**1**
			4	**Лабораторне заняття**	*Лабораторна робота 8*. Розгортання та управління інфраструктурою відкритих ключів	Захист лабораторної роботи	**5**
		СРС	**6**	**Підготовка до занять**	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до лабораторного заняття		
Здатність виконувати оцінювання криптостійкості на основі методів криптоаналізу	**10**	**Аудиторні**	**2**	**Лекція**	*Тема 10.* Основні види атак, принципи криптоаналізу. Основи криптоаналізу	Активна участь на занятті	**1**
			4	**Лабораторне заняття**	*Лабораторна робота 8.* Розгортання та управління інфраструктурою відкритих ключів		
		СРС	**4**	**Підготовка до занять**	Підготовка до заліку		
Усього годин		**120**		**Загальна максимальна кількість балів**			**100**

Отримання балів студентами денної форми навчання за темами змістових модулів здійснюється за схемою, наведеною в табл. 10.2.

Таблиця 10.2

Розподіл балів за темами

Поточне тестування та самостійна робота															Сума
Змістовий модуль 1									Змістовий модуль 2						
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т12	Т13	Т14	Т15	100
6	5	6	9	9	3	3	22	11	6	3	3	6	7	1	

Максимальна кількість балів, яку може накопичити студент протягом тижня за формами та методами навчання, наведена в табл. 10.3.

Таблиця 10.3

Розподіл балів за тижнями

Теми змістових модулів				Лекційні заняття	Захист лабораторних робіт	Експрес-опитування	Поточні КР	Усього
Змістовий модуль	1	Тема 1	1 тиждень	1	5	–	–	6
		Теми 2, 3	2 тиждень	1	5	5	–	11
		Теми 4, 5	3 тиждень	1	5	–	12	18
		Теми 6, 7	4 тиждень	1	5	–	–	6
		Тема 8	5 тиждень	1	5	4	–	10
		Теми 11, 12	6 тиждень	1	5	–	12	18
	2	Тема 9	7 тиждень	1	5	5	–	11
		Теми 13, 14	8 тиждень	1	5	–	–	6
		Тема 10	9 тиждень	1	–	–	12	13
		Тема 15	10 тиждень	1	–	–	–	1
Усього				**10**	**40**	**14**	**36**	**100**

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 ЄКТС (табл. 10.4).

Таблиця 10.4

Переведення показників успішності знань студентів ХНЕУ ім. С. Кузнеця в систему оцінювання за шкалою ECTS

Сума балів за всіма видами навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

11. Рекомендована література

11.1. Основна

1. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – Москва : СОЛОН-Прес, 2002. – 272 с.

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

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

4. Остапов С. Е. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці : ВД "Родовід", 2014. – 428 с.

11.2. Додаткова

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

6. 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.

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

8. Столлингс В. Криптография и защита сетей: принципы и практика / В. Столлингс ; пер. с англ. – 2-е изд. – Москва : ИД "Вильямс", 2001. – 672 с.

9. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. – Киев : Юниор, 2003. – 504 с.

11.3. Ресурси мережі Internet

10. Журнал "Информационные технологии. Аналитические материалы". – Режим доступа : http://it.ridne.net.

11. Центр информационных технологий. – Режим доступа : http://www.citmgu.ru.

12. Історія розвитку інформаційних технологій в Україні. – Режим доступу : http://www.icfcst.kiev.ua/MUSEUM/IT_u.html.

13. Нормативные акты Украины. – Режим доступа : www.nau.kiev.ua.

14. Information Technology Security Evaluation Criteria. – V. 1.2. – Office for Official publications of the European Communities, 1991. – Access mode : www.fbi.gov.

Додатки

Додаток А
Таблиця А.1

Структура складових професійних компетентностей з навчальної дисципліни "Захист інформації" за Національною рамкою кваліфікацій України

Складові компетентності, яка формується в рамках теми	Мінімальний досвід	Знання	Уміння	Комунікації	Автономність і відповідальність
1	2	3	4	5	6
Змістовий модуль 1. Безпека та захист даних					
Тема 1. Огляд безпеки системи					
Здатність визначати основні поняття про систему безпеки. Основні вимоги щодо секретної системи. Основи криптоаналізу простих шифрів	Знання основних положень міжнародних і національних стандартів щодо безпеки інформації	Знання основних понять, послуг і механізмів їх забезпечення на основі міжнародних і національних стандартів щодо безпеки інформації	Провести загальне оцінювання функціонування КСіМ за основними критеріями безпеки	Презентувати результати визначення криптостійкості простих шифрів	Відповідальність за точність і коректність результатів
Тема 2. Механізми та політики розмежування прав доступу					
Здатність ставити завдання, аналізувати, давати порівняльну характеристику різних режимів застосування алгоритмів блокового шифрування	Знання основних вимог до використання режимів роботи БСШ	Знання основних вимог до побудови та порівняльних характеристик БСШ, їх режимів застосування. Формування політик розмежування прав доступу	Провести загальне оцінювання функціонування БСШ у різних режимах використання, проаналізувати можливість ПЗ щодо розмежування права доступу	Презентувати результати визначення основних показників за критеріями оцінки БСШ, використання в різних режимах	Відповідальність за точність і коректність результатів
Тема 3. Методи та пристрої забезпечення захисту та безпеки					
Здатність ставити завдання, аналізувати, давати порівняльну характеристику різних режимів застосування алгоритмів блокового шифрування	Знання основних вимог щодо використання режимів роботи БСШ	Знання основних вимог до побудови та порівняльних характеристик БСШ, режимів їх застосування. Формування політик розмежування прав доступу	Провести загальне оцінювання функціонування БСШ у різних режимах використання, проаналізувати можливість ПЗ щодо розмежування прав доступу	Презентувати результати визначення основних показників за критеріями оцінки БСШ, використання в різних режимах	Відповідальність за точність і коректність результатів

1	2	3	4	5	6
Тема 4. Захист, доступ та автентифікація					
Здатність ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів асиметричного шифрування на прикладі алгоритму *RSA*. Основні протоколи його використання	Знання основних вимог щодо використання процедур несиметричного шифрування	Знання основних вимог до побудови та порівняльних характеристик алгоритмів несиметричної криптографії. Вимоги й основні процедури побудови геш-функцій	Провести загальне оцінювання функціонування несиметричних криптосистем і процедур формування *MAC* і *MDC*-кодів	Презентувати результати використання алгоритмів несиметричної криптографії або використання *MAC* і *MDC*-кодів щодо формування послуг автентифікації та доступності	Відповідальність за точність і коректність результатів
Тема 5. Моделі захисту. Захист пам'яті					
Здатність визначати основні поняття про електронний підпис (ЦП). Основні вимоги щодо його формування та використання в сучасних протоколах	Знання основних вимог щодо використання процедур несиметричного шифрування	Знання основних вимог до побудови та порівняльних характеристик алгоритмів несиметричної криптографії. Вимоги й основні процедури побудови геш-функцій	Провести загальне оцінювання функціонування несиметричних криптосистем і процедур формування *MAC* і *MDC*-кодів в протоколах ЦП	Презентувати результати використання алгоритмів несиметричної криптографії або використання *MAC* і *MDC*-кодів щодо формування послуг автентифікації	Відповідальність за точність і коректність результатів
Тема 6. Шифрування даних					
Здатність ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів асиметричного шифрування на прикладі алгоритму *RSA*. Основні протоколи його використання	Знання основних вимог щодо використання процедур симетричного та несиметричного шифрування	Знання основних вимог до побудови та порівняльних характеристик алгоритмів несиметричної та симетричної криптографії. Вимоги й основні процедури побудови шифр-текстів	Провести загальне оцінювання функціонування симетричних і несиметричних криптосистем	Презентувати результати використання алгоритмів симетричної та несиметричної криптографії	Відповідальність за точність і коректність результатів
Тема 7. Управління відновленням					
Здатність визначати основні поняття про електронний підпис. Основні вимоги щодо його формування та використання в сучасних протоколах автентифікації	Знання основних вимог щодо використання процедур цифрового підпису	Знання основних вимог до побудови та порівняльних характеристик алгоритмів геш-функцій та процедури ЦП	Провести загальне оцінювання функціонування несиметричних криптосистем і процедур формування *MAC* і *MDC*-кодів в протоколах ЦП	Презентувати результати використання алгоритмів несиметричної криптографії або використання *MAC*- і *MDC*-кодів у формуванні послуг автентифікації	Відповідальність за точність і коректність результатів

1	2	3	4	5	6
Тема 8. Основні напрями розвитку сучасної криптографії					
Здатність визначати основні поняття про сучасні протоколи втаємничення інформації на основі цифрової стеганографії. Основні вимоги щодо стегасистеми	Знання основних процедур втаємничення даних на основі методів цифрової стеганографії	Знання й основні принципи використання методів приховування інформації за допомогою методів цифрової стеганографії, використання алгоритмів із застосуванням на еліптичних кривих	Провести загальне оцінювання функціонування стеганосистем і процедур приховування інформації в сучасних цифрових каналах	Презентувати результати використання алгоритмів цифрової стеганографії у забезпеченні приховування факту, часу, місця й інформаційного посилання	Відповідальність за точність і коректність результатів
Тема 9. Механізми та протоколи управління ключами в ІВК інформаційної системи					
Здатність визначати основні поняття про PKI. Життєвий цикл сертифікатів ключів	Знання основних процедур і центрів в PKI	Знання основних протоколів, процедур та архітектури PKI, механізми забезпечення формування та сертифікації ключів	Провести загальне оцінювання функціонування основних центрів і процедур у протоколах PKI, механізмів сертифікації ключів	Презентувати результати використання механізмів і протоколів PKI, життєвого циклу ключів	Відповідальність за точність і коректність результатів
Змістовий модуль 2. Мережева безпека					
Тема 10. Основні види атак, принципи криптоаналізу. Основи криптографії					
Здатність визначати основні поняття про основні види атак, принципи криптоаналізу (диференційного та лінійного). Моделі порушника	Знання основних принципів сучасних процедур криптоаналізу	Знання основ проведення диференційного та лінійного криптоаналізу, сучасні процедури розпаралелювання процедур атаки "грубої сили", основи класифікації загроз на сучасні КМ	Проведення оцінювання криптостійкості на основі основних процедур диференційного та лінійного криптоаналізу	Презентувати результати використання процедур диференційного та лінійного криптоаналізу	Відповідальність за точність і коректність результатів
Тема 11. Алгоритми із секретним ключем					
Здатність визначати основні алгоритми системи захищеної електронної пошти *PGP*, функції, алгоритми та механізми. Система формування й обміну ключами	Знання основних вимог щодо використання режимів роботи БСШ, формування поточних шифрів	Знання основних вимог до побудови та порівняльних характеристик БСШ і поточних симетричних систем, режимів їх застосування. Основи криптостойкості, моделі секретних систем	Провести загальне оцінювання функціонування БСШ в різних режимах використання, аналіз сучасних алгоритмів симетричної криптографії	Презентувати результати визначення основних показників за критеріями оцінки БСШ, поточних алгоритмів шифрування, використання в різних режимах	Відповідальність за точність і коректність результатів

Закінчення табл. А.1

1	2	3	4	5	6
Тема 12. Алгоритми з відкритим ключем					
Здатність визначати основні алгоритми системи захищеної електронної пошти *PGP*, функції, алгоритми та механізми	Знання основних вимог щодо використання процедур симетричного та несиметричного шифрування.	Знання основних вимог до побудови та порівняльних характеристик алгоритмів несиметричної криптографії. Основи криптостойкості. Моделі секретних систем	Провести загальне оцінювання функціонування несиметричних криптосистем	Презентувати результати використання алгоритмів несиметричної криптографії	Відповідальність за точність і коректність результатів
Тема 13. Протоколи автентифікації					
Здатність визначати основні протоколи автентифікації, основних функцій та протоколів систем PKI, *IPSec, SSL (TLS)*	Знання основних протоколів у сучасних системах глобальних мереж	Знання основних механізмів і протоколів систем PKI, *IPSec*, *SSL* (*TLS*) із забезпечення основних послуг безпеки даних у глобальних обчислювальних мережах	Проведення порівняльного аналізу механізмів і протоколів забезпечення основних послуг безпеки даних у глобальних обчислювальних мережах	Презентувати результати порівняльного аналізу механізмів і протоколів забезпечення основних послуг безпеки	Відповідальність за точність і коректність результатів
Тема 14. Цифрові підписи					
Здатність визначати основні протоколи автентифікації, основних функцій та протоколів систем PKI, *IPSec, SSL (TLS)*	Знання основних процедур сучасних механізмів ЦП	Знання основних механізмів і процедур побудови сучасних ЦП у протоколах систем PKI, *IPSec*, *SSL* (*TLS*)	Проведення порівняльного аналізу процедур ЦП систем PKI, *IPSec*, *SSL* (*TLS*)	Презентувати результати порівняльного аналізу ЦП систем PKI, *IPSec*, *SSL* (*TLS*)	Відповідальність за точність і коректність результатів
Тема 15. Використання паролів і механізмів контролю за доступом					
Здатність визначати основні поняття про основні види атак, принципи криптоаналізу. Моделі порушника	Знання основних принципів сучасних процедур криптоаналізу	Знання основ проведення диференційного та лінійного криптоаналізу, сучасні процедури розпаралелювання процедур криптоаналізу	Проведення оцінювання криптостійкості на основі основних процедур диференційного та лінійного криптоаналізу	Презентувати результати використання процедур диференційного та лінійного криптоаналізу	Відповідальність за точність і коректність результатів

Додаток Б

Зразок екзаменаційного білета

Харківський національний економічний університет імені Семена Кузнеця
Освітній ступінь "бакалавр"
Напрям підготовки: "Комп'ютерні науки". Семестр VIII
Навчальна дисципліна "Захист інформації"

ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № 1

1. Яке з наведених визначень є визначенням криптографії?

а. Прикладна інженерно-технічна дисципліна, яка займається розробленням, аналізом і обґрунтуванням стійкості криптографічних засобів захисту інформації від загроз з боку супротивника.

б. Галузь дискретної математики або математичної кібернетики, що вивчає математичні моделі криптографічних схем.

в. Завдання щодо порушення конфіденційності, цілісності, невідстежуваності криптографічного протоколу, що стоїть перед супротивником.

г. Наука про протидію захисту інформації у персональних комп'ютерах.

2. Що з наведеного є визначенням прикладного криптографічного протоколу?

а. Протокол, який використовується або потенційно може використовуватися для вирішення практичних задач.

б. Протокол, який не має самостійного прикладного значення, але використовується як компонент для побудови більш складних прикладних криптографічних протоколів.

в. Основний тип криптографічних протоколів, призначених для забезпечення цілісності. Є два основні різновиди – протокол автентифікації учасника (протокол автентифікації або протокол ідентифікації) та протокол автентифікації повідомлень.

г. Протокол, який використовується або потенційно може використовуватися для вирішення теоретичних завдань.

3. Що з наведеного визначень є визначенням криптології?

а. Прикладна інженерно-технічна дисципліна, яка займається розробленням, аналізом і обґрунтуванням стійкості криптографічних засобів захисту інформації від загроз з боку противника, вирішуючи тим самим три завдання криптографії – забезпечення конфіденційності, цілісності, невідстежуваності.

б. Галузь дискретної математики або математичної кібернетики, що вивчає математичні моделі криптографічних схем.

в. Завдання щодо порушення конфіденційності, цілісності криптографічного протоколу, що стоїть перед противником.

г. Протокол, який не має самостійного прикладного значення, але використовується як компонент для побудови більш складних прикладних криптографічних протоколів.

4. Якої групи вірусів не існує?

а. Завантажувальної.

б. Файлової.

в. Файлово-текстової.

г. Поліморфної.

5. Який із симптомів не пов'язаний з вірусним зараженням ПК?

а. Уповільнення роботи деяких програм.

б. Збільшення розмірів текстових файлів.

в. Поява не існуючих раніше дивних файлів.

г. Самовільне перезавантаження комп'ютера.

6. Яка з програм не є антивірусною?

а. Програма-фаг.

б. Програма-ревізор.

в. Програма-фільтрат.

г. Програма-імунізатор.

7. Комп'ютерний вірус – це?

а. Спеціально написана програма, здатна самовільно приєднуватися до інших програм, створювати свої копії та впроваджувати їх у файли, системні області комп'ютера і в обчислювальні мережі з метою порушення роботи програм, псування файлів і каталогів, створення всіляких перешкод у роботі комп'ютера.

б. Спеціальний програмно-апаратний комплекс, здатний самовільно приєднуватися до інших програм, створювати свої копії та впроваджувати їх у файли, системні області комп'ютера і в обчислювальні мережі з метою порушення роботи програм, псування файлів і каталогів, створення всіляких перешкод в роботі комп'ютера.

в. Спеціальна системна програма, здатна самовільно приєднуватися до інших програм, створювати свої копії та впроваджувати їх у файли, заподіювати псування файлів і каталогів, створювати всілякі перешкоди в роботі комп'ютера.

г. Програма, яка спотворює файли комп'ютера та видаляє інформацію про користувача.

8. У функції центру управління ключовою системою не входить?

а. Створення ключів.

б. Створення сертифікатів.

в. Створення алгоритмів електронних цифрових підписів.

г. Управління ключами.

9. Як називають структуру служби безпеки України, що займається захистом інформації?

а. ФАПСІ.

б. ДСТСЗІ.

в. ЦРО.

г. МАССАД.

10. Який з алгоритмів не належить до класу геш-функцій?

а. MD 5.

б. SHA.

в. MH 4.

г. MD 4.

2. Зашифруйте за допомогою шифру Цезаря з ключовим словом відкритий текст. *Відкритий текст:* автентичність. *Ключ(і):* пам'ять. *Алфавіт(и): український.*

3. Побудуйте протокол обміну інформації між користувачами А та В за допомогою алгоритму несиметричного шифрування *RSA* для забезпечення КОНФІДЕНЦІЙНОСТІ (структурна схема протоколу з визначенням процедур шифрування/розшифрування та ключів абонентів). Визначити переваги та недоліки даного протоколу. Порівняйте з протоколами на основі гешування.

4. Ви є користувачем розподіленої захищеної системи з шістьма користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (розшифрування) *RSA* та створювати або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувачі	Параметри системи n		Ключі користувачів	
	p	q	Особливий (секретний) d	Відкритий (публічний) e
A	11	13	17	
B	17	19		11
C	11	17	13	
D	13	19		89
E	17	23	19	
F	13	17		109

Ви користувач "B".
Перевірте, що ваші ключі (відкритий і особливий) відібрані правильно.
Розшифруйте повідомлення M, яке отримано від користувача "C".

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	Геш-значення	ЦП
Шифрування *RSA*	C	B	8	–	–

Затверджено на засіданні
кафедри інформаційних систем ХНЕУ ім. С. Кузнеця.
Протокол №___ від "___" _____ 20____р.

Зав. кафедри _____ Екзаменатор _____.
(підпис) (підпис)

Зміст

НАВЧАЛЬНЕ ВИДАННЯ

Робоча програма
навчальної дисципліни
"ЗАХИСТ ІНФОРМАЦІЇ"

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

Самостійне електронне текстове мережеве видання

Укладачі: **Євсеєв** Сергій Петрович
Король Ольга Григорівна

Відповідальний за видання *В. В. Чубук*

Редактор *Н. І. Ганцевич*

Коректор *О. С. Новицька*

План 2016 р. Поз. № 114 ЕВ. Обсяг 50 с.

Видавець і виготовлювач – ХНЕУ ім. С. Кузнеця, 61166, м. Харків, просп. Науки, 9-А

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру
ДК № 4853 від 20.02.2015 р.