МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Робоча програма

навчальної дисципліни

"ІНФОРМАЦІЙНА БЕЗПЕКА"

для студентів напряму підготовки "Комп'ютерні науки"

усіх форм навчання

Харків. Вид. ХНЕУ, 2008

Затверджено на засіданні кафедри інформаційних систем.

Протокол №2 від 28.09.2005 р.

Р78 Робоча програма навчальної дисципліни "Інформаційна безпека" для студентів напряму підготовки "Комп'ютерні науки" усіх форм навчання / Укл. С. В. Кавун. – Харків: Вид. ХНЕУ, 2007. – 44 с. (Укр. мов.).

Подано тематичний план навчальної дисципліни та її зміст за модулями й темами, вміщено плани лекції і лабораторних занять, методичні рекомендації, роботи щодо закріплення знань та система оцінювання студентів. Робоча програма складена на основі Державного освітнього стандарту вищої освіти за напрямом "Комп'ютерні науки".

Рекомендовано для студентів V курсу спеціальностей "Інформаційні управляючі системи та технології" та "Комп'ютерний еколого-економічний моніторинг" усіх форм навчання.

Вступ

Навчальну дисципліну "Інформаційна безпека" віднесено до групи професійно-практичних дисциплін підготовки спеціалістів за спеціальностями "Інформаційні управляючи системи та технології" і "Комп'ютерний еколого-економічний моніторинг". Вона є невід'ємною частиною циклу комп'ютерних дисциплін, необхідних працівникам підприємств незалежно від форми власності та організаційно-правової форми господарювання.

Вивчення дисціплини "Інформаційна безпека" дозволяє студентам оволодіти знаннями та вміннями, які утворять теоретичний і практичний фундамент, необхідний для побудови й аналізу безпечних інформаційних систем і технологій у галузі оброблення інформації в автоматизованих інформаційних системах із застосуванням різноманітних режимів роботи ЕОМ й проходить на п'ятому курсі в дев'ятому семестрі.

Метою навчальної дисципліни є навчання студентів принципам організації та забезпечення інформаційної безпеки в комп'ютерних мережах та системах, розглядаючи їх як комплекс технічних, інформаційних та програмних засобів, що призначені для вирішення широкого кола завдань забезпечення безпеки інформаційних процесів; формування необхідних теоретичних знань та практичних навичок у галузі побудови та функціонування систем інформаційної безпеки (ІБ) і комп'ютерних технологій та можливостей їх використання.

Предмет навчальної дисципліни – логічні, інформаційні та архітектурні основи побудови ІБ інформаційних процесів та систем різних рівнів, призначення і принципів дії основних модулів та їх взаємозв'язок.

Теоретичними та науковими основами дисципліни є алгебра логіки, теорія алгоритмів, теорія інформації та комп'ютерні мережі та системи.

Методичною основою дисципліни є методи аналізу, моделювання та синтезу інформаційних процесів у системах ІБ, які базуються на математичному апараті теорії графів, теорії імовірності та математичної статистики.

Спосіб досягнення зазначеної мети міститься у використанні в навчально-виховному процесі системи педагогічних заходів та дій, що

засновані на реалізації під час занять загальнодидактичних принципів інформаційно-рецептивного, репродуктивного та проблемного методів навчання.

Структура робочої програми навчальної дисципліни "Інформаційна безпека" наведена в табл. 1.

Таблиця 1

Структура програми навчальної дисципліни

<table>
<tr><td>Навчальна дисципліна: підготовка спеціалістів</td><td>Напрям, спеціальність, освітньо-кваліфікаційний рівень</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Кількість кредитів відповідних ECTS: 3 кредити,
у тому числі: змістовних модулів – 2, самостійна робота; індивідуальне навчально-дослідне завдання (ІНДЗ);
завдання для самостійної роботи</td><td>Назва напряму
"Комп’ютерні науки"</td><td>Вибіркова.
Рік підготовки: 5.
Семестр: 9</td></tr>
<tr><td>Кількість годин усього – 108,
за змістовними модулями:
модуль 1 – 72 години,
модуль 2 – 36 годин.</td><td>Назви спеціальностей:
"Інформаційні управляючі системи та технології"
"Комп’ютерний еколого-економічний моніторинг"</td><td rowspan="2">Лекції (теоретична підготовка): 18 годин.

Лабораторні роботи: 18 годин.

Самостійна робота: 54 години.

ІНДЗ: 18 годин</td></tr>
<tr><td rowspan="2">Кількість тижнів викладання – 18
Кількість годин за тиждень – 5</td><td rowspan="2">Освітньо-кваліфікаційний рівень:
спеціаліст</td></tr>
<tr><td>Вид контролю:
ПМК</td></tr>
</table>

Основними завданнями в процесі вивчення дисципліни є: одержання знань з основоположних принципів побудови та функціонування системи ІБ операційних систем; одержання знань про архітектуру побудови системи ІБ, функціональні можливості модулів ІБ та їх управлінням; підготовка студента до подальшого поглибленого вивчення ІБ, її функціонування; вироблення навичок самостійного

вивчення різних систем ІБ інформаційних процесів та проведення її порівняльного аналізу при створенні ефективного програмного забезпечення.

Засобами досягнення мети та рішення завдань дисципліни є:

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

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

Навчальна дисципліна базується на знаннях та вміннях, отриманих при вивченні дисциплін "Архітектура ЕОМ", "Системне програмування та операційні системи", "Комп'ютерні мережі" і забезпечує підготовку студента за фахом.

Необхідним елементом успішного засвоєння навчального матеріалу дисципліни є самостійна робота студентів з літературою з питань ІБ і технологій її побудови.

У процесі навчання студенти отримують необхідні знання під час проведення аудиторних занять: лекційних, практичних та 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 інформаційних систем і технологій

Дисципліна "Інформаційна безпека" є вибірковою для підготовки спеціалістів технічних 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 галузі інформатики та комп'ютерної техніки, фахових курсів з адміністрування ОС.

У свою чергу знання з даної дисципліни забезпечують успішне виконання курсових і дипломних проектів.

У результаті вивчення запропонованої навчальної дисципліни студенти повинні знати:

1. Тенденції розвитку науки та техніки в області ІБ, актуальні проблеми теорії ІБ.

2. Основні терміни та визначення, принципи побудови та функціонування ІБ.

3. Основні принципи організації й алгоритми функціонування систем безпеки в сучасних ОС і оболонках.

4. Можливості застосування в роботі сучасних системних програмних засобів: ОС, операційних оболонок, що обслуговують програми.

5. Основні принципи організації й алгоритми функціонування ОС і оболонок.

6. Проблеми й напрямки розвитку системних програмних засобів.

7. Способи організації ІБ, режими роботи мереж та робочих станцій різних класів.

8. Методи аналізу мережної активності та створення оптимальних умов управління ІБ.

9. Способи організації політики безпеки при організації комп'ютерних мереж та систем, особливості її використання.

Практичні навички, якими оволодівають студенти при вивченні навчальної дисципліни:

1. Орієнтуватися в різних архітектурних рішеннях побудови ІБ інформаційних процесів, особливо у сферах їх застосування.

2. Ставити завдання, давати порівняльну характеристику різних варіантів рішення організації ІБ.

3. Оформлювати прийняті рішення у вигляді комплекту технічної документації, враховувати технологічні, ергономічні та естетичні фактори під час розробки системи безпеки різного рівня.

4. Проводити об'єктивний аналіз ефективності прийнятих технічних рішень, користуватися обраним математичним апаратом щодо вирішення інженерних та наукових завдань, які виникають під час розробки та дослідження ІБ.

5. Розробляти та будувати ефективну політику безпеки в організації та на підприємстві.

Програму навчальної дисципліни розроблено у відповідності до вимог галузевого стандарту вищої освіти на базі освітньо-професійної програми підготовки спеціаліста. Враховано рекомендації положень

Болонської декларації щодо кредитно-модульної системи організації навчального процесу.

Програма дисципліни відповідає вимогам державного стандарту освіти з напряму "Комп'ютерні науки".

2. Тематичний план навчальної дисципліни

При вивченні дисципліни "Інформаційна безпека" студент має ознайомитися з програмою дисципліни, її структурою, формами та методами навчання, видами і методами контролю знань.

Тематичний план дисципліни "Інформаційна безпека" складається з двох модулів, кожний з яких об'єднує в собі відносно окремий самостійних блок дисципліни, який логічно пов'язує кілька навчальних елементів дисципліни за змістом та взаємозв'язками.

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

Таблиця 2

Структура залікового кредиту навчальної дисципліни

Тема	Кількість годин, відведених на				
	лекції	лабораторні заняття	практичні заняття	самостійну роботу	ІНДЗ
1	2	3	4	5	6
Змістовний модуль 1. Основи інформаційної безпеки					
Тема 1. Загальні принципи безпеки інформаційних технологій	2	2		12	4
Тема 2. Канали витоку інформації	4	4		12	4
Тема 3. Організація інформаційної безпеки на підприємстві	6	8		10	4
Змістовний модуль 2. Особливості застосування ІБ у бізнесі					
Тема 4. Організація інформаційної безпеки комп'ютерних мереж	4	4		10	3
Тема 5. Правові основи ІБ	2			10	3
Усього	18	18		54	18

3. Зміст навчальної дисципліни за модулями та темами

МОДУЛЬ 1. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ТЕМА 1. Загальні принципи безпеки інформаційних технологій

Поняття інформації та її захисту. Основні поняття захисту інформації: речова, телекомунікаційна та документована. Інформаційні ресурси й процеси. Категорії інформації: державна таємниця, комерційна, службова та банківська таємниця, персональна інформація.

Поняття національної безпеки. Види ІБ. ІБ у системі національної безпеки України. Загальнометодологічні принципи теорії ІБ. Державна інформаційна політика. Проблеми регіональної ІБ. Методи й засоби забезпечення ІБ.

Основні характеристики інформації: конфіденційність, цілісність та доступність. Методи порушення конфіденційності, цілісності й доступності інформації.

Загрози ІБ, їх класифікація та основні характеристики. Уразливість інформації. Основні групи загроз: порушення цілісності, порушення конфіденційності та доступності інформації. Аналіз погроз ІБ, проблеми інформаційної війни.

Існуючі стандарти ІБ, їх основні положення щодо використання в інформаційних технологіях. Нормативні документи на підприємстві для організації безпеки інформаційних технологій. Основні заходи щодо організації спеціального діловодства з носіями інформації.

Роботи, які пов’язані із розробкою й аналізом засобів забезпечення ІБ комп’ютерних систем на основі розроблених програм і методик, у тому числі із забезпеченням вимог, що випливають із документів, що регламентують режим дотримання державної таємниці.

Аналіз існуючих методів і засобів, застосовуваних для контролю й захисту інформації, і розробка пропозицій щодо їхнього вдосконалення й підвищення ефективності.

Оцінка техніко-економічного рівня й ефективності запропонованих і реалізованих організаційно-технічних рішень, пов’язаних із застосуванням програмно-технічних засобів ІБ, з урахуванням перспектив та напрямків їхнього вдосконалення.

ТЕМА 2. Канали витоку інформації

Історичний аспект виникнення та використання каналів витоку інформації.

Поняття каналу витоку інформації. Класифікація каналів витоку інформації, їх характеристики. Сфери використання каналів витоку інформації. Методи та засоби захисту каналів витоку інформації.

Поняття інформаційного потоку в каналі витоку інформації. Математичний опис інформаційного потоку.

Способи використання каналів витоку інформації в процесі діяльності підприємства.

Таємні канали витоку інформації. Організація виявлення таємних каналів витоку інформації. Моделі таємних каналів витоку інформації. Організація захисту інформації при визначенні таємних каналів витоку інформації.

Загальні класифікація віддалених мережних атак при використанні електронних каналів витоку інформації. Типові віддалені атаки. Атаки на основі використання стеку протоколів TCP/IP.

Основи використання сканерів ІБ в різних каналах витоку інформації. Властивості, достоїнства та недоліки використання сканерів ІБ. Аналіз інформації, отриманої при використанні сканерів ІБ.

Організація проведення різних видів аудиту інформації в різних каналах витоку інформації. Аналіз та подальше використання інформації, отриманої при проведенні аудиту. Формування "динаміки" використання каналів витоку інформації з метою отримання оцінки їх ефективності.

ТЕМА 3. Організація інформаційної безпеки на підприємстві

Поняття політики безпеки (ПБ) на підприємстві. Приклади розроблених ПБ на підприємстві. Служби ІБ на підприємстві. Типові функціональні обов’язки співробітників служби ІБ. Методика розробки ПБ на підприємстві. Основні етапи реалізації ПБ в умовах сучасного бізнесу. Приклади сценаріїв злому ІС на підприємстві.

Багаторівнева структура ПБ. Математичний опис багаторівневої ПБ. Політика захисту цілісності Байба.

Типова структура підсистеми безпеки ОС і функції, які виконуються: ідентифікація й аутентифікація, розмежування доступу, аудит, підзвітність дій, повторне використання об'єктів, точність і надійність обслуговування, захист обміну даних. Реалізація підсистеми ІБ на підприємстві.

Відомі міжнародні стандарти управління ІБ: BS 7799 (ISO/IEC 17799 и ISO/IEC 27001), Orange Book, X.800, критерії Європейських держав, Control Objectives for Information and Related Technology (COBIT), IT Infrastructure Library (ITIL) и Statement on Auditing Standards (SAS) No. 70, керівні документи Держтехкомісії Росії.

Архітектура систем попередження вторгнення – Intrusion Prevention Systems (IPS). Організація конфігурування IPS для подальшого використання на підприємстві.

Архітектура систем визначення вторгнення – Intrusion Detection Systems (IDS). Організація конфігурування IDS для подальшого використання на підприємстві.

Організація використання обох систем – IPS та IDS для забезпечення комплексного захисту.

Організація оптимального використання парольного захисту інформації на підприємстві.

Властивості, достоїнства та недоліки використання парольного захисту.

Розрахунок стійкості парольного захисту інформації. Використання парольного захисту інформації в різних системах.

Організація на підприємстві групи влагоджування інцидентів комп'ютерної безпеки (ГУІКБ). Її права, статус, обов'язки.

Порядок й організація проведення розслідування за фактом комп'ютерного інциденту.

Системи аутентифікації та ідентифікації. Класифікація систем аутентифікації та ідентифікації. Особливості електронних систем аутентифікації та ідентифікації.

МОДУЛЬ 2. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІБ У БІЗНЕСІ

ТЕМА 4. Організація інформаційної безпеки комп'ютерних мереж

Програмно-апаратні засоби забезпечення ІБ в комп'ютерних мережах. Протоколи аутентифікації при вилученому доступі. Засоби й методи забезпечення цілісності й конфіденційності. Захист серверів та робочих станцій. Засоби захисту локальних мереж при підключенні до Інтернет. Захисні екрани. Захист віртуальних локальних мереж.

Організація ІБ мережі за допомогою брандмауерів та фаєрволів. Проектування правил брандмауерів. Апаратні реалізації брандмауерів та фаєрволів.

ІБ при роботі в мережі Інтернет. Типи ресурсів та сервісів у мережі Інтернет, які використовуються на підприємствах. ІБ при роботі із електронної поштою. Організація ІБ від несанкціонованого доступу при роботі із ресурсами ICQ, IRC, CHAT. Організація ІБ робочого місця працівника підприємства при роботі в мережі Інтернет. Використання програмних засобів запобігання несанкціонованого доступу.

Використання технології захисту мережі – IPSec. Організація захисту каналів зв'язку за допомогою IPSec. Достоїнства IPSec. Організація настроювання служб IPSec. Технологія роботи IPSec. Архітектура IPSec.

ТЕМА 5. Правові основи ІБ

Законодавство України в області ІБ, захисту державної таємниці й конфіденційної інформації. Види інформації, що захищається. Державна таємниця як особливий вид інформації, що захищається. Конфіденційна інформація. Система захисту державної таємниці. Правовий режим захисту державної таємниці. Ліцензійна й сертифікаційна діяльності в області ІБ. Правові основи захисту інформації із використанням застосування технічних засобів (захисту від технічних розвідок, застосування й розробка шифрувальних засобів і т. д.). Захист інтелектуальної власності засобами патентного й авторського права.

Правова регламентація охоронної діяльності. Міжнародне законодавство в області ІБ. Злочини у сфері комп'ютерної інформації. Експертиза злочинів в області комп'ютерної інформації. Криміналістичні аспекти проведення розслідувань.

Наслідки порушення ІБ на підприємстві. Основні закони та положення України, які регламентують відповідальність за порушення ІБ.

Правовий статус ГУІКБ на підприємстві. Юридичний аспект функціонування ГУІКБ на підприємстві. Відповідальність членів ГУІКБ.

4. Плани лекцій

МОДУЛЬ 1. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ТЕМА 1. Загальні принципи безпеки інформаційних технологій

1.1. Завдання та зміст навчальної дисципліни.
1.2. Основні поняття та стандарти ІБ.
1.3. Класифікація загроз ІБ. Основні характеристики інформації.

Література: основна [2 – 4]; додаткова [2; 4; 5; 9 – 11].

ТЕМА 2. Канали витоку інформації

2.1. Класифікація каналів витоку інформації.
2.2. Методи та засоби захисту каналів витоку інформації.
2.3. Таємні канали витоку інформації.
3.1. Класифікація віддалених мережних атак.
3.2. Сканери ІБ та їх характеристики.
3.3. Методика проведення аудиту.

Література: основна [2; 3]; додаткова [1; 4; 10].

ТЕМА 3. Організація інформаційної безпеки на підприємстві

4.1. Організація політики безпеки (ПБ) на підприємстві.
4.2. Методика розробки ПБ на підприємстві.
4.3. Багаторівнева структура ПБ.

5.1. Типова структура підсистеми безпеки ОС.

5.2. Міжнародні стандарти управління ІБ.

5.3. Організація оптимального використання парольного захисту інформації на підприємстві.

6.1. Системи аутентифікації та ідентифікації.

6.2. Системи попередження вторгнення – Intrusion Prevention Systems (IPS).

6.3. Системи визначення вторгнення – Intrusion Detection Systems (IDS).

Література: основна [1 – 4]; додаткова [2; 3; 5; 7; 8; 12].

МОДУЛЬ 2. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІБ У БІЗНЕСІ

ТЕМА 4. Організація інформаційної безпеки комп'ютерних мереж

7.1. Програмно-апаратні засоби забезпечення ІБ в комп'ютерних мережах.

7.2. Протоколи аутентифікації при вилученому доступі.

7.3. Захист віртуальних локальних мереж.

8.1. Організація ІБ мережі за допомогою брандмауерів та фаєрволів.

8.2. ІБ при роботі в мережі Інтернет.

8.3. Технологія захисту мережі – IPSec.

Література: основна [1; 3; 4]; додаткова [4; 5; 7; 11; 12].

ТЕМА 5. Правові основи ІБ

9.1. Законодавство України в області ІБ.

9.2. Міжнародне законодавство в області ІБ.

9.3. ГУІКБ на підприємстві.

Література: основна [1 – 3]; додаткова [9, 13, 15, 16].

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.

Лабораторні заняття проводяться в спеціально обладнаних навчальних лабораторіях з використанням устаткування, пристосованого до умов навчального процесу (лабораторні макети, установки тощо).

В окремих випадках лабораторні заняття можуть проводитися в умовах реального професійного середовища (наприклад, у школі, на виробництві, в наукових лабораторіях).

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.

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 виставленні поточної модульної (практичний модульний контроль) оцінки з даної навчальної дисципліни.

Перелік тем лабораторних занять наведений в табл. 3.

Таблиця 3

Перелік тем лабораторних занять

	Теми лабораторних занять	Кількість годин
1	2	3
Модуль 1. Основи інформаційної безпеки	1. Дослідження систем визначення атак (СВА) та типів мережних атак	4
	2. Ознайомлення із типовою апаратурою зйому інформації за технічними каналами витоку даних	2
	3. Дослідження можливостей системи аналізу та управління інформаційними ризиками: гриф (з програмного комплексу Digital Security Office 2006). Побудова моделі ІС на основі моделі інформаційних потоків	4
	4. Перехоплення даних аутентифікації SMB, проникнення в комп'ютерну систему під управлінням ОС Windows NT/2000/XP/2003	4
Модуль 2. Особливості застосування ІБ у бізнесі	5. Дослідження можливостей системи розробки та управління ПБ ІС підприємства на основі стандарту ISO 17799: КОНДОР (з програмного комплексу Digital Security Office 2006). Розрахунок ризиків невиконання вимог стандарту ISO 17799	4

При проведенні ЛР студент повинен продемонструвати:

творчий підхід до дослідження тематики адміністрування і моніторингу;

грамотне використання існуючого програмного забезпечення;

навички висококваліфікованого конфігурування і використання відповідних програмних засобів та додатків.

Студент повинен уміти встановити, конфігурувати й правильно використовувати програмний продукт, використовувати якісний аналіз отриманих параметрів і характеристик, виконувати оцінку отриманих результатів. Велике значення має графічне представлення отриманого матеріалу (у вигляді screensave-ів) з описом і поясненнями до використовуваного додатка.

Виконання ЛР містить такі етапи:

1. Підготовчий етап (до проведення ЛР):

а) одержання відповідного даним методичним рекомендаціям 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 (при необхідності), 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.

6. Індивідуальне навчально-дослідне завдання

Індивідуальне навчально-дослідне завдання (ІНДЗ) виконується самостійно при консультуванні викладачем протягом вивчення дисципліни у відповідності 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 вирішенні проблем адміністрування на підприємстві за допомогою впровадження інформаційних систем і технологій.

Індивідуальне навчально-дослідне завдання припускає наявність наступних елементів наукового дослідження: практичної значущості; комплексного системного підходу до вирішення завдань дослідження; теоре-

тичного використання передової сучасної методології і наукових розробок; наявність елементів творчості.

Практична значущість 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.

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 інформаційної системи і 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 її удосконалення, окремих задач обробки інформації, студент повинен використовувати відомості про новітню обчислювальну техніку і інформаційні технології, запропонувати автоматизоване рішення задачі моніторингу цих показників.

У процесі виконання ІНДЗ, разом з теоретичними знаннями і практичними навичками за фахом, студент повинен продемонструвати здіб-ності до науково-дослідної роботи і вміння творчо мислити, навчитися вирішувати науково-прикладні актуальні задачі.

6.1. Тематика ІНДЗ

Тема ІНДЗ за дисципліною "Інформаційна безпека" є однаковою для всіх студентів, але виконується для певної задачі моніторингу показників на матеріалах підприємств – баз практики. У випадках, коли декілька студентів проходили практику на одному підприємстві, тема ІНДЗ може змінюватися або уточнюватися за розсудом викладача.

Тема ІНДЗ: "Розроблення постановки задачі "<назва задачі визначення показників ефективності функціонування ІБ>", алгоритму її розв’язання з використанням відомих засобів моніторингу та аудиту".

Мета роботи: Розроблення елементів автоматизованої інформаційної системи визначення показників ефективності функціонування ІБ.

Основні завдання:

1. Розроблення постановки задачі визначення показників ефективності функціонування ІБ.
2. Розроблення алгоритму оброблення інформації за задачею визначення показників ефективності функціонування ІБ.
3. Розроблення довідника користувача з рішення задачі.

6.2. Вимоги до змісту ІНДЗ

ІНДЗ повинне містити наступні розділи.

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

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 розділів.

Перший розділ повинен містити постановку задачі – необхідну і достатню сукупність відомостей щодо конкретної задачі визначення показників ефективності функціонування ІБ, які визначають її сутність. У цьому розділі студент повинен визначити:

1. Характеристику задачі – призначення задачі, перелік об’єктів при управлінні якими вирішується задача; періодичність і тривалість вирішення умови, за яких призупиняється автоматизоване розв’язання задачі; зв’язки задачі іншими задачами; посади осіб, що визначають умови вирішення задачі; розподіл дій між персоналом і технічними засобами.
2. Вихідні повідомлення – перелік і опис вихідних повідомлень (ідентифікатор, форма подання повідомлень і вимоги до неї; періодичність видавання, термін видавання та час за який має бути прийнято рішення; користувачі і призначення вихідної інформації), а також перелік та опис

структурних одиниць (назва, ідентифікатор вихідного повідомлення, що містить одиницю; вимоги до точності та надійності обчислень).

3. Вхідні повідомлення – перелік і опис вхідних повідомлень (ідентифікатор, форма подання повідомлень; термін і частота надходження повідомлення), а також перелік та опис структурних одиниць (назва, потрібна точність її числового значення, джерело інформації).

Другий розділ повинен містити інформацію щодо опису алгоритму розв'язання задачі, який включає: призначення і характеристику; використовувану інформацію, результати розв'язування, математичний опис, алгоритм розв'язування в табличному або графічному вигляді.

Третій розділ повинен містити результати розроблення довідника користувача як складової технологічного забезпечення.

Довідник користувача складається з наступних підрозділів: вступ (сферу застосування; короткий опис можливостей; рівень підготовки користувача; перелік експлуатаційної документації, з якою необхідно ознайомитися користувачу); призначення й умови застосування; підготовка до роботи; опис операцій; аварійні ситуації; рекомендації з освоєння.

Висновки. У висновках викладають перелік і рекомендацій та практичні результати, одержані в ІНДЗ. Далі формулюють висновки щодо практичного використання здобуття результатів.

Список літератури. Джерела розміщувати в 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 студентів

Необхідним елементом успішного засвоєння навчального матеріалу дисципліни є самостійна робота студентів з вітчизняною та закордонною

спеціальною технічною літературою, нормативними актами з питань адміністрування та моніторингу. Самостійна робота є основним засобом оволодіння навчальним матеріалом у час, вільний від обов'язкових навчальних занять. Основні види самостійної роботи, які запропоновані студентам:

1. Вивчення лекційного матеріалу.
2. Робота з вивчення рекомендованої літератури.
3. Вивчення основних термінів та понять галузі ІБ.
4. Підготовка до семінарських і практичних занять, дискусій, роботи в малих групах.
5. Підготовка до проміжного та підсумкового контролю.
6. Контрольна перевірка кожним студентами особистих знань за питаннями для самостійного поглибленого вивчення та самоконтролю.
7. Робота над рефератом.

7.1. Питання для самостійного опрацювання

МОДУЛЬ 1. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ТЕМА 1. Загальні принципи безпеки інформаційних технологій

Питання для самостійного поглибленого вивчення

1. Дайте визначення інформації, її категорії.
2. Визначіть мету використання державної інформаційної політики.
3. У чому полягають принципові відмінності різних категорій інформації?
4. Що дозволяє виявити використання існуючих стандартів ІБ?
5. Назвіть основні принципи побудови ІБ.
6. Назвіть основні загрози ІБ.
7. Дайте визначення національної безпеки.
8. Опишіть загальнометодологічні принципи теорії ІБ.

Теми рефератів

1. Організація державної інформаційної політики.
2. Аналіз існуючих методів і засобів, застосовуваних для контролю й захисту інформації, і розробка пропозицій щодо їхнього вдосконалення й підвищення ефективності.

Основна література: [2 – 4].

Додаткова: [2; 4; 5; 9 – 11].

ТЕМА 2. Канали витоку інформації

Питання для самостійного поглибленого вивчення

1. Опишіть історію виникнення та використання каналів витоку інформації.
2. Визначте поняття каналу витоку інформації та їх класифікацію.
3. У чому полягають принципові відмінності різних каналів витоку інформації.
4. Опишіть основні характеристики таємних каналів витоку інформації.
5. Основні характеристики сканерів ІБ.
6. Методика проведення різних видів аудиту інформації в різних каналах витоку інформації.

Теми рефератів

1. Технічні канали витоку інформації.
2. Методика визначення каналів витоку інформації.
3. Сутність інформаційного потоку в каналі витоку інформації.
4. Типові віддалені атаки.

Основна література: [2; 3].

Додаткова: [1; 4; 10].

ТЕМА 3. Організація інформаційної безпеки на підприємстві

Питання для самостійного поглибленого вивчення

1. Визначіть мету використання ПБ на підприємстві.
2. Опишіть процес розробки ПБ на підприємстві.
3. Дайте визначення політики захисту цілісності Байба.
4. У чому полягають принципові відмінності міжнародних стандартів управління ІБ?
5. Області використання систем попередження вторгнення.
6. Назвіть основні принципи побудови систем визначення вторгнення.

7. Наведіть класифікацію систем аутентифікації та ідентифікації.

Теми рефератів

1. Характеристика технічних засобів IDS.
2. Характеристика програмного забезпечення парольного захисту інформації на підприємстві.
3. Характеристика групи улагоджування інцидентів комп'ютерної безпеки (ГУІКБ).

Основна література: [1 – 4].
Додаткова: [2; 3; 5; 7; 8; 12].

МОДУЛЬ 2. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІБ У БІЗНЕСІ

ТЕМА 4. Організація інформаційної безпеки комп'ютерних мереж

Питання для самостійного поглибленого вивчення

1. Дайте визначення протоколу аутентифікації при вилученому доступі.
2. Дайте визначення цілісності й конфіденційності.
3. Дайте визначення вразливості.
4. Класифікуйте основні типи брандмауерів та фаєрволів.
5. У чому полягають принципи захисту віртуальних локальних мереж?
6. Області використання програмних засобів запобігання несанкціонованого доступу.
7. Назвіть основні принципи побудови технології захисту мережі – IPSec.

Теми рефератів

1. Склад інформаційної бази брандмауерів та фаєрволів.
2. Призначення та зміст ІБ при роботі із електронної поштою.

Основна література: [1; 3; 4].
Додаткова: [4; 5; 7; 11; 12].

ТЕМА 5. Правові основи ІБ

Питання для самостійного поглибленого вивчення

1. Дайте визначення видів інформації, що належать для захисту.

2. Дайте визначення державної таємниці.

3. У чому полягають принципові відмінності ліцензійної й сертифікаційної діяльності в області ІБ?

4. Області використання патентного й авторського права.

5. Основні закони та положення України, які регламентують відповідальність за порушення ІБ.

6. Юридичний аспект функціонування ГУІКБ на підприємстві.

Теми рефератів

1. Міжнародне законодавство в області ІБ.

2. Криміналістичні аспекти проведення розслідувань.

Основна література: [1 – 3].

Додаткова: [1; 4; 5; 11].

7.2. Тематика контрольних робіт для студентів заочної форми навчання

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.

Завдання 1

Вивчіть запропоновані сканери ІБ, визначіть, при цьому, їх основні можливості, параметри та характеристики. Також за допомогою запропонованого сканера ІБ визначте існуючу модель ІБ на об’єкті, ктрий підлягає дослідженню.

Отримати за допомогою запропонованого сканера ІБ згідно з заданим варіантом існуючу вразливість на об’єкті, котрий підлягає дослідженню. При цьому провести детальне дослідження та отримати звіт, який необхідно навести в контрольної роботі. Дослідження можливо проводити або на підприємстві, або на віртуальної системі.

Номери варіантів завдань для дослідження наведені в табл. 5.

Таблиця 5

Варіанти завдання для дослідження

Сканер / Тип Дослідження	PC Security Test; EnterpriseScan-x86; TestHttp	Shadow Security Scaner	CyberCop Scanner	Webtrends Security Analyzer Pro	GFI LANguard Network Security Scanner (LNSS)	NESSUS	XSpider	MS Baseline Security Analyzer (MBSA)	Nikto; Entry	N.E.W.T.	Retina® Network Security Scanner
Сканування робочої станції	1	2	3	4	5	6	7	8	9	10	11
Сканування сервера	12	13	14	15	16	17	18	19	20	21	22
Сканування діапазону IP-адрес	23	24	25	26	27	28	29	30	31	32	33

Завдання 2

1. Використовуючи ПЗ за заданим варіантом (табл. 6) провести дослідження парольного захисту відповідних типів об’єктів системи ІБ.

2. У процесі дослідження побудувати графіки залежності швидкості й часу аудиту пароля від їхньої складності й довжини (обмежитися максимальною довжиною при великому алфавіті до 5 символів) для **всіх** досліджуваних програм.

3. Для **LC5**: для наведених файлів .SAM (.SAM1) визначити паролі і їхню складність для зазначених користувачів, результат показати у вигляді скриншоту.

4. Для **Advanced PDF Password Recovery PRO**: для наведених файлів Security.pdf (Security1.pdf) визначити паролі та їхню складність, результат показати у вигляді скриншоту.

5. Для **PDF**: створити власні варіанти паролів на файли заданого типу (.pdf) і вказати їхню складність.

6. Для **Active Password Changer**: створити 3-х користувачів із правами адміністратора та оригінальними паролями для кожного. Також створити завантажувальний носій і помістити на неї зазначену програму – pwd_chng.exe. За допомогою отриманого носія зробити завантаження ОС. Виконати наступні операції: відобразити всі облікові записи в системі; відключити одного зі створених користувачів; скинути пароль

другого користувача; для третього користувача встановити або скинути прапори "Перемінити пароль при наступному вході", "Пароль ніколи не минає", "Акаунт відключений", установивши їх для даного користувача попередньо у відповідні значення. Усі результати виконання підтвердити скриншотами.

7. Для **ZIP**: для наведених файлів kavun.zip (Sec.zip) визначити паролі і їхню складність, результат показати у вигляді скриншоту.

8. Для **PPA**: для наведених файлів .SAM (.SAM1) провести аналогічне дослідження з аналогії з п. 3, результат показати у вигляді скриншоту.

9. Для **Advanced Office Password Recovery**: для наведеного файлу Sec.doc визначити пароль і його складність, результат показати у вигляді скриншоту. Провести аналогічне дослідження для інших типів документів з офісного пакета, попередньо створивши приклади файлів самостійно.

10. Для **KeyLoggers**: зробити установку й настроювання програми. Зробити показ (скриншот) перехоплених паролів користувачів при вході в систему й інші варіанти введення пароля на інші додатки зі збереженого файлу.

Таблиця 6

Варіанти завдань

ПЗ / № варианта	LC5	Advanced PDF Password Recovery PRO	PDF	Active Password Changer	ZIP	PPA	Advanced Office Password Recovery	Key Loggers
1.	+	+		+	+			+
2.	+		+	+		+		+
3.	+	+		+			+	+
4.	+		+	+	+			+
5.	+	+		+		+		+
6.	+		+	+			+	+
7.	+	+		+	+			+
8.	+		+	+		+		+
9.	+	+		+			+	+
10.	+		+	+	+			+
11.	+	+		+		+		+
12.	+		+	+			+	+
13.	+	+		+	+			+
14.	+		+	+		+		+
15.	+	+		+			+	+
16.	+		+	+	+			+
17.	+	+		+		+		+
18.	+		+	+			+	+
19.	+	+		+	+			+

№ варианта \ ПЗ	LC5	Advanced PDF Password Recovery PRO	PDF	Active Password Changer	ZIP	PPA	Advanced Office Password Recovery	Key Loggers
20.	+		+	+		+		+
21.	+	+		+			+	+
22.	+		+	+	+			+
23.	+	+		+		+		+
24.	+		+	+			+	+
25.	+	+		+	+			+
26.	+		+	+		+		+
27.	+	+		+			+	+
28.	+		+	+	+			+
29.	+	+		+		+		+
30.	+		+	+			+	+

Завдання 3

1. Ознайомтесь із роботою наступних утиліт:

SMBRelay; LC; RPC GUI;

2. Вивчить захисні заходи, які необхідні для нейтралізації досліджуваних атак.

3. Вивчивши роботу утиліт, здійсніть наступне.

Перехоплення хешів паролів, за допомогою запуску на своїй машині помилкового SMB-сервера, і відправлення спеціального поштового повідомлення із впровадженим дескриптором зображення. Перехопіть за таким способом 3 – 4 паролі. Проведіть відповідні захисні заходи й повторіть спробу перехоплення паролів. Спробуйте розшифрувати перехоплені паролі. Протестуйте внутрішню комп’ютерну мережу (робочу станцію) навчального класу на наявність уразливості переповнення буфера служби RPC. При виявленні уразливості на одному з комп’ютерів підключитеся до нього й, експлуатуючи вразливість, заведіть на вилученому ПК обліковий запис із правами адміністратора. Створіть на вилученому комп’ютері розподілений ресурс. Впровадьте на вилучений комп’ютер програмну закладку (наприклад, створіть тунельоване з’єднання за допомогою утиліти NetCAT) із використанням FTP. Повторите пункти 3.5 – 3.6 після реалізації контрзаходів щодо усунення уразливості переповнення буфера служби RPC.

4. Зробіть висновки.

5. Усі отримані результаті в ході проведеного дослідження необхідно підтвердити відповідними результатами у вигляді скриншотів.

8. Контрольні запитання для самодіагностики

МОДУЛЬ 1. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ТЕМА 1. Загальні принципи безпеки інформаційних технологій

1. У чому полягають принципові відмінності категорій інформації.
2. Причини використання ПБ.
3. Назвіть основні принципи побудови теорії ІБ.
4. Назвіть типи загроз ІБ.
5. Назвіть існуючі стандарти ІБ.

Література: основна [2 – 4]; додаткова [2; 4; 5; 9 – 11].

ТЕМА 2. Канали витоку інформації

1. Що дозволяє виявити використання каналів витоку інформації?
2. Назвіть основні принципи побудови каналів витоку інформації.
3. Назвіть типи таємних каналів витоку інформації.

Література: основна [2; 3]; додаткова [1; 4; 10].

ТЕМА 3. Організація інформаційної безпеки на підприємстві

1. Дайте визначення ПБ.
2. Дайте визначення систем попередження вторгнення.
3. У чому полягають принципові відмінності систем визначення вторгнення?
4. Області використання систем аутентифікації та ідентифікації.
5. Назвіть основні принципи міжнародних стандартів управління ІБ.
6. Назвіть типи устаткування, використовувані в ПБ.

Література: основна [1 – 4], додаткова [2; 3; 5; 7; 7; 8; 12].

МОДУЛЬ 2. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІБ У БІЗНЕСІ

ТЕМА 4. Організація інформаційної безпеки комп’ютерних мереж

1. Назвіть типи протоколів аутентифікації.
2. Дайте визначення брандмауера.
3. Дайте визначення фаєрвола.
4. У чому полягають принципові відмінності брандмауерів та фаєрволів?
5. Області використання технології захисту мережі – IPSec.
6. Назвіть основні принципи побудови програмних засобів запобігання несанкціонованого доступу.
7. Назвіть типи брандмауерів та фаєрволів.

Література: основна [1; 3; 4]; додаткова [4; 5; 7; 11; 12].

ТЕМА 5. Правові основи ІБ

1. Назвіть основні принципи побудови ліцензійної й сертифікаційної діяльності в області ІБ.
2. Назвіть закони та положення України, які регламентують відповідальність за порушення ІБ.
3. Назвіть області використання патентного й авторського права.
4. Назвіть достоїнства ГУІКБ на підприємстві.

Література: основна [1 – 3], додаткова [1; 4; 5; 11].

9. Індивідуально-консультативна робота

Індивідуально-консультативні заняття (ІКЗ) – вид навчальних занять, 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 і закріплення знань з окремих питань та тем дисциплін, надання методичної допомоги у виборі раціональних методів самостійної роботи. При необхідності можуть проводитись і групові ІКЗ.

Відвідання ІКЗ студентами добровільне. Проте кафедри можуть викликати на співбесіду тих студентів, які в процесі навчання не показують твердих знань і, на думку викладачів, не працюють над вивченням дисципліни. Консультуючи студентів, викладач одночасно знайомиться з тим, як вони вивчають рекомендовану літературу, дає поради та рекомендації 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 в ході ІКЗ, не повинні впливати на екзаменаційну або залікову оцінку.

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

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

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

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

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

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

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

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

1) індивідуального захисту самостійних та індивідуальних завдань;

2) підготовки рефератів для виступу на науковому семінарі,

3) підготовки рефератів для виступу на науковій конференції.

10. Методики активізації процесу навчання

При викладенні дисципліни "Інформаційна безпека" 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. 7.

Таблиця 7

Розподіл форм та методів активізації процесу навчання за темами навчальної дисципліни

Тема	**Практичне застосування навчальних технологій**
1	2
ТЕМА 1. **Загальні принципи безпеки інформаційних технологій**	Кейс "Структура системи ІБ на підприємстві"
ТЕМА 2. **Канали витоку інформації**	Міні-лекція "Методика визначення та технічних каналів витоку інформації"
ТЕМА 3. **Організація інформаційної безпеки на підприємстві**	Проблемна лекція з питання вибору інформаційних технологій для створення ефективної ІБ на підприємстві. Ділова гра "Обґрунтування вибору інформаційних технологій для створення ефективної ІБ на підприємстві"
ТЕМА 4. **Організація інформаційної безпеки комп'ютерних мереж**	Проблемна лекція з питання "Організація конфігурування брандмауерів та файерволів, які розташовані на базі сервера". Презентація результатів роботи в малих групах
ТЕМА 5. **Правові основи ІБ**	Проблемна лекція "Обґрунтування вибору ГУІКБ"

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 щодо питань, які 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 активізуючу роль, примушує студентів сконцентруватися і почати активно мислити в пошуках правильної відповіді.

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

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

Семінари-дискусії – передбачають обмін думками і поглядами учасників з приводу даної теми, а також розвивають мислення, допомагають формувати погляди і 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 як омога більшу кількість ідей за невеликий проміжок 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 та 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 адміністрування та моніторингу інформаційних систем підприємства.

Оцінювання знань, умінь та навичок студентів враховує види занять, які згідно з програмою навчальної дисципліни "Інформаційна безпека" передбачають лекційні, практичні та лабораторні заняття, а також самостійну роботу і виконання індивідуальних завдань.

Перевірка та оцінювання знань студентів може проводитися кількома методами:

1. Оцінювання знань студента під час лабораторних та практичних занять.
2. Оцінювання виконання індивідуального навчально-дослідного завдання.
3. Написання рефератів.
4. Виконання завдань для самостійної роботи.
5. Проведення проміжного контролю.

6. Проведення поточно-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 модульних оцінок та оцінки за результатами підсумкового контролю.

Порядок поточного оцінювання знань студентів. Поточне оцінювання здійснюється під час проведення лабораторних занять і має на меті 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 обробблення облікової інформації, розробленні постановки задачі, алгоритму та технології її розв’яза, 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 всім п’ятьом

зазначеним критеріям. Відсутність тієї або іншої складової знижує оцінку на відповідну кількість балів.

При оцінюванні індивідуальних завдань увага також приділяється якості, самостійності та своєчасності здачі виконаних завдань викладачу (згідно з графіком навчального процесу). 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 "Інформаційна безпека". Мета реферату – поглиблення теоретичних знань, набутих студентами в процесі вивчення дисципліни.

Написання реферату має сприяти глибшому засвоєнню студентами дисципліни "Інформаційна безпека", спонукає ґрунтовно вивчати нормативно-законодавчу базу, статистичні матеріали, спеціальні наукові видання вітчизняних і закордонних авторів, у яких розглядаються питання впровадження та ефективного використання інформаційних систем і технологій.

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 в 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 або інші питання і проблеми з теми дослідження.

План має включати лише ті питання, які безпосередньо стосуються теми і дають змогу повно і 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, курс, номер академічної групи; дата подання реферату викладачу на перевірку (день, місяць, рік).

За титульним аркушем слідує детальний план реферату, у 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 куті сторінки, при цьому нумерація починає ставитися на першому аркуші після вступу.

У кінці реферату дається повний список використаних джерел. Його необхідно скласти в 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 і 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 бали) — 9 – 7 правильних відповідей;

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

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

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

Метою вирішення тестових завдань з навчальної дисципліни "Інформаційна безпека" є засвоєння студентами теоретичних знань з ІБ в середовищі певної інформаційної системи з використанням інформаційних технологій, 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 і евристичних), згідно з якими 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. Структура білетів з модульного контролю аналогічна структурі білетів 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.

Таким чином після вивчення тем 1 – 3 (модуль 1) студенти денної форми виконують завдання до модуля 1. Відповідно, після вивчення тем 4 – 5 (модуль 2) – завдання до модуля 2.

Завдання модульного контролю містить 2 завдання з лекційного модуля та 3 завдання з практичного модуля (стереотипне, діагностичне та евристичне).

Зразок завдання до модуля 1

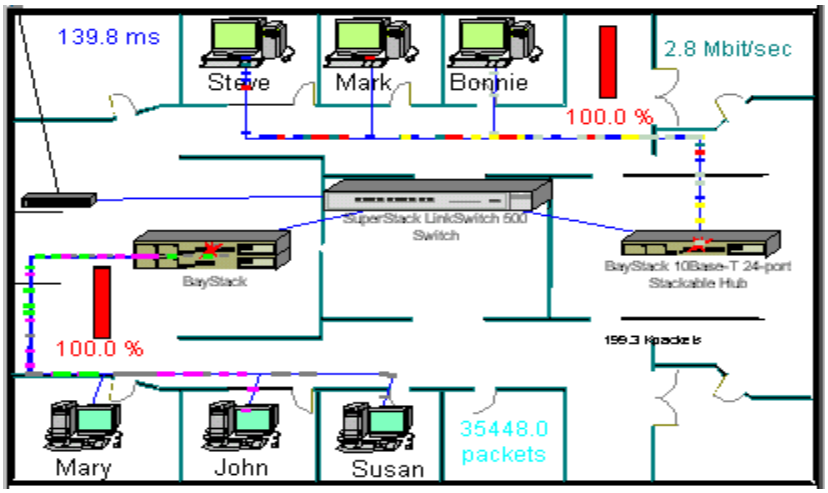
Теоретична частина

1. Охарактеризувати забезпечуючі підсистеми ІБ.
2. Тестові завдання одиничного і множинного вибору.

Практична частина

Завдання 1 (стереотипне). Навести приклади організаційних дій при розробці системи ІБ на підприємстві.

Завдання 2 (діагностичне). Визначити всі елементи логічної та фізичної структури в наведеній мережі при формуванні топологічної схеми в структурі ПБ.



Завдання 3 (евристичне).

Розробити ПБ на підприємстві.

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 ІБ, 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 ІБ, 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 завдання є правильним, але припущені неточності в розробленні певних питань з організації ІБ) або не зовсім повних висновків щодо одержаних результатах вирішення завдання. 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 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.

Для підведення підсумків роботи студентів з навчальної дисципліни "Інформаційна безпека" виставляється загальна оцінка,

яка враховує оцінки за кожним видом контролю (дві оцінки поточно-модульного контролю за роботу протягом семестру та оцінка за результатами підсумкового контролю).

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. 8).

Таблиця 8

Переведення показників успішності знань студентів у 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
10	виконання задовольняє мінімальні критерії	E	5 – 4	
–	потрібне повторне перескладання	FX	3	незадовільно
–	повторне вивчання дисципліни	F	2 – 1	

12. Рекомендована література

12.1. Основна

1. Англо-український тлумачний словник з обчислювальної техніки, Інтернету і програмування. – Вид. 1. – К.: Вид. дім "Софт Прес", 2005. – 552 с.

2. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К.: ООО "ТИД "ДС", 2001. – 688 с.

3. Олейников Е. А. Экономическая и национальная безопасность: Учебник для вузов / Рос. экон. акад. им. Г. В. Плеханова. – М.: Экзамен, 2005. – 766 с.

4. Рассел Ч. Microsoft Windows 2000 Server. Справочник администратора / Ч. Рассел, Ш. Кроуфорд [Пер. с англ. – 2-е изд., испр. – М.: Изд. "ЭКОМ", 2002. – 1296 с.

5. Симонович С. В. INTERTET: Лаборатория мастера: Практическое пособие по эфективным приемам работы в Интернете / С. В. Симонович, Г. А. Евсеев, В. И. Мураховский – М.: АСТ-ПРЕСС: Инфорком-Пресс, 2000. – 720 с.

12.2. Додаткова

1. Закон України "Про захист інформації в автоматизованих системах" // Відомості Верховної ради України. – 1994. – №31.

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

3. Гроувер Д. Защита программного обеспечения: Пер. с англ. / Под ред. Д. Гроувера. – М.: Свет, 1992. – 280 с.

4. Європа на шляху до інформаційного суспільства: Збірник документів Європейської Комісії 1994 – 1995 рр. – К.: Державний комітет зв’язку та інформатизації України, 2000.

5. Д. П. Зегжда Как построить защищенную информационную систему / Ивашко А. М.; [Под науч. ред. Д. П. Зегжды . и В. В. Платонова. – Спб.: Свет и родина – 95, 1997. – 312 с.

6. Ибе О. Сети и удаленный доступ. Протоколы, проблемы, решения. – М.: ДМК Пресс, 2002. – 336 с.

7. Іванов В. Ф. Інформаційне законодавство: український та зарубіжний досвід / Київський ун-т ім. Т. Г. Шевченка. Інститут журналістики. – К., 1999. – 208 с.

8. Люцарев В. С. Безопасность компьютерных сетей на основе Windows NT / В. С. Люцарев, К. В. Ермаков, Е. Б. Рудный, И. В. Ермаков –М.: Издательский отдел "Русская Редакция" ТОО "Channel Trading Ltd.", 1998. – 304 с.

9. Microsoft Corporation. Безопасность сети на основе Microsoft Windows 2000. Учебный курс MCSE: Пер. с англ. – М.: Издательско-торговый дом "Русская редакция", 2001. – 912 с.

10. Соколов А. В., Методи информационной защиты объектов и компьютерных сетей / А. В. Соколов, Степанюк О. М. – М.: ТОВ "Фирма "Издательство АСТ"; ТОВ "Издательство "Полигон", 2000. – 272 с.

11. Филин С. А. Информационная безопасность: Учебное пособие. – М.: Изд. "Альфа-Пресс", 2006. – 412 с.

12. Rainbow Series. DoD Trusted Computer Systems Evaluation Criteria /DoD 5200.28 STD - Orange Book.

12.3. Ресурси мережі Internet

1. http://bezopasnost.biz.

2. http://dstszi.gov.ua.

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

2. Центр информационных технологий. – http://www.citmgu.ru

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

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

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

7. www.fbi.gov.

8. www.pgpi.org.

9. www.rootshell.com.

10. www.securityfocus.com.
11. www.sysinternals.com.
12. www.zdnet.ru.
13. www.submarine.ru.
14. www.securitylab.ru.

Зміст

НАВЧАЛЬНЕ ВИДАННЯ

Робоча програма
навчальної дисципліни
"ІНФОРМАЦІЙНА БЕЗПЕКА"
для студентів напряму підготовки "Комп'ютерні науки"
усіх форм навчання

Укладачі: **Кавун Сергій Віталійович**

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

Редактор **Анацька О. В.**

Коректор

План 2008 р. Поз. №228.

Підп. до друку Формат 60 × 90 1/16. Папір MultiCopy. Друк Riso.

Ум.-друк. арк. 4,0. Обл.-вид. арк. 4,6. Тираж прим. Зам. №

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

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

Робоча програма
навчальної дисципліни

"ІНФОРМАЦІЙНА БЕЗПЕКА"

для студентів напряму підготовки "Комп'ютерні науки"
усіх форм навчання