

МІЖРЕГІОНАЛЬНА  
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ



МАУП



**НАВЧАЛЬНА ПРОГРАМА**  
дисципліни  
**“ІНФОРМАЦІЙНІ МЕРЕЖІ”**  
(для магістрів)

**МАУП**

Київ 2008

Підготовлено доцентом кафедри інформатики та інформаційних технологій  
*В. М. Ахрамовичем*

Затверджено на засіданні кафедри інформатики  
та інформаційних технологій (протокол № 15 від 18.10.07)

*Схвалено Вченою радою Міжрегіональної Академії управління персоналом*



**Ахрамович В. М.** Навчальна програма дисципліни “Інформаційні мережі” (для магістрів). – К.: МАУП, 2008. – 22 с.

Навчальна програма містить пояснювальну записку, тематичний план, зміст дисципліни “Інформаційні мережі”, завдання для контрольних робіт, питання для самоконтролю, а також список рекомендованої літератури.

© Міжрегіональна Академія  
управління персоналом (МАУП), 2008

## ПОЯСНЮВАЛЬНА ЗАПИСКА

Інформаційні мережі — це фундаментальна підготовка у сфері проектування мереж для передачі великих потоків інформації і з великою швидкістю, вирішення завдань маршрутизації цих потоків, забезпечення високої якості передачі інформаційних даних, управління і синхронізації мережі загалом і кожної її ланки зокрема, використання цифрових систем та інтелектуальних комп'ютерних технологій.

Інформаційна мережа — спільне підключення багатьох окремих комп'ютерів (робочих станцій, серверів різних типів) до каналів передачі даних, з метою отримання чи обробки необхідної інформації у потрібному режимі. Для створення мережі потрібно поєднати в єдине ціле комп'ютери, мережеве обладнання (апаратне забезпечення) та мережеве системне програмне забезпечення. Для створення автоматизованої інформаційної системи на основі мережі потрібно додати прикладне ПЗ, інформаційне, організаційне та інші види забезпечення. В сучасних умовах динамічно розвивається ринок комп'ютерних мереж, які дають змогу проводити розподільчу обробку інформації та її отримання в інтерактивному та асинхронному режимах. При вирішенні управлінських, економічних та інших типів задач, істотного значення для спеціалістів набуло вміння застосовувати ресурси та можливості сучасних мережних комп'ютерних програм, мереж різних рівнів, інформаційних технологій. Однак для того, щоб повною мірою використовувати можливості обчислювальної техніки та мереж, треба ці можливості знати, вміти користуватися новими програмними продуктами, ресурсами комп'ютерних мереж, проектувати мережі.

Інформаційні мережі в економіці та управлінні дають змогу використовувати комплекс методів та засобів оперативного отримання та переробки початкових даних у вірогідну інформацію для прийняття рішень на основі програмних та апаратних засобів комп'ютерних мереж із метою досягнення оптимальних ринкових параметрів об'єкта управління.

Вивчення дисципліни “Інформаційні мережі” сприяє формуванню у студентів системи знань у галузі теорії та практики застосування та проектування сучасних мереж різних рівнів, програмних продуктів, технічних засобів у сфері управлінської діяльності.

**Мета** вивчення дисципліни “Інформаційні мережі”:

- формування системи фундаментальних знань щодо аналізу та проектування:

- локальних мереж (для офісних та корпоративних інформаційних систем (ІС));
- глобальних ІС, у тому числі систем Internet/Intranet, каналів та мережного обладнання в Internet/Intranet;
- управління мережними інформаційними ресурсами.

У результаті вивчення дисципліни студенти повинні:

- знати базові мережні інформаційні технології і сервіси;
- набути теоретичних знань та практичних навичок у сфері проектування та застосування мережних інформаційних технологій і сервісів, а також набуття практичних навичок аналізу, побудови та використання, захисту від несанкціонованого доступу до інформації;
- опанувати сучасні технології розробки і менеджменту мережних інформаційних систем і ресурсів.

Предмет дисципліни: методологія проектування та використання локальних і глобальних мереж для офісних і корпоративних ІС.

**Завданням** дисципліни є вироблення у студентів практичних навичок проектування та використання сучасних мережних інформаційних технологій і сервісів для вирішення інформаційних потреб організації. Вказані мережні інформаційні технології розглядаються як невід’ємний компонент технологій Інтернет/Intranet.

### **Місце дисципліни та її значення у навчальному процесі**

У сучасному суспільстві для задоволення його потреб виникають проблеми інформаційного забезпечення усіх сфер діяльності людини. Особливо стрімко в останні роки розвиваються інформаційні мережі, що спричинено потребами суспільства у різних галузях людської діяльності. Актуальне питання підготовки спеціалістів з інформаційних мереж, які могли б задовольнити потреби суспільства. Викладання навчальної дисципліни має забезпечити:

- вивчення архітектури комп’ютерних мереж, програмного забезпечення та методів їх проектування; набуття практичних навичок аналізу, побудови та використання, захисту несанкціонованого доступу до інформації;
- отримання знань про мережні операційні системи, системи управління базами даних, локальні та глобальні комп’ютерні мережі, а також вміння застосовувати перелічені засоби для вирішення конкретних завдань.

## **Міждисциплінарні зв'язки**

Цей курс ґрунтується на знаннях, отриманих студентами у процесі вивчення курсів: “Інформатика та комп'ютерна техніка”, “Архітектура комп'ютерів”, “Основи Інтернет технологій”, “Технології і засоби адміністрування комп'ютерних мереж”, “Методи та засоби комп'ютерних інформаційних технологій”, “Технології мультимедіа”, “Технологія програмування та створення програмних продуктів”, “Організація баз даних та баз знань”, “Комп'ютерні мережі” та ін. Вивчення дисципліни сприятиме кращому розумінню предмета при вивченні наступних навчальних дисциплін: “Апаратне та програмне забезпечення дистанційного навчання”, “Програмне забезпечення автоматизованих систем”, “Використання пакетів прикладних програм” та ін.

Під час вивчення курсу передбачається систематична практична робота студентів за комп'ютерами як під керівництвом викладача, так і самостійно.

Передбачено постійний контроль вивчення дисципліни (захист лабораторних робіт, опитування на лекціях) та періодичний контроль (контроль знань за кожним модулем, періодичні тестування, залік за дисципліну).

### **ТЕМАТИЧНИЙ ПЛАН дисципліни “ІНФОРМАЦІЙНІ МЕРЕЖІ”**

№ пор.	Назва змістового модуля і теми
1	<b>Змістовий модуль I. Менеджмент інформаційних мереж</b>
2	Об'єднання мереж
2	Технології мереж
3	<b>Змістовий модуль II. Менеджмент інформаційної безпеки</b>
3	Мережні операційні системи
4	Захист мереж
Разом годин: 108	

## ***ЗМІСТ ДИСЦИПЛІНИ “ІНФОРМАЦІЙНІ МЕРЕЖІ”***

### **Змістовий модуль I. Менеджмент інформаційних мереж**

#### ***Тема 1. Об'єднання мереж***

Організації, які займаються стандартизацією мереж. Еталонна модель Open Systems Interconnections (OSI) та її рівні. Ієрархічний зв'язок. Формати інформації. Проблеми сумісності. Адресація, блоки даних, пакети.

Визначення маршруту та компоненти маршрутизації. Типи і метрики алгоритмів маршрутизації та комутації.

Порівняння устроїв для об'єднання мереж. Основи технології об'єднання мереж. Типи мостів. Прозоре та трансляційне об'єднання мереж за допомогою мостів. Петлі, алгоритм зв'язуючого дерева. Алгоритм Source-Route Bridging (SRB).

Архітектура управління мережею ISO. Управління конфігурацією, ресурсами, захистом даних.

Порівняння мереж Ethernet, TELENET, TYMNET, Token Ring та IEEE 802.3, LocalTalk. Фізичне підключення, формати блоків, передача маркера. Пріоритети, управління несправностями.

Розрахунок Ethernet та FastEthernet мереж. Управління протоколами.

*Література* [1; 3–6; 12–15; 34; 38; 39]

#### ***Тема 2. Технології мереж***

Основи технології, технічні умови, фізичне з'єднання, комутація та інкапсуляція, типи трафіка, формати блока даних, особливості стійкості мережі, послуги, рівні FDDI, UltraNet, ISDN.

Концентратори, мережні процесори, адаптери каналів зв'язку, програмне забезпечення, корпоративна та глобальна адресація, маршрутизація та її рівні.

Технологія оптоволоконних систем. Електронні компоненти.

Fiber Distributed Data Interface, протоколи управління каналами зв'язку PPP (LCP), Synchronous Data-Link Control, HDLC, LAP, LAPB, Logical Link Control, CCITT Recommendation X.25, Frame Relay, SMDS, DQDB, SIP, DNA, XNS, IPX, CMIP, XNS протокол доставки дейтаграм DDP, протокол підтримки маршрутної таблиці RTMP, протокол транзакцій ATP, протокол потоку даних ADSP,

протокол маршрутизації DECnet Phase IV, IS-IS, RIP, протокол з'єднання PPP, протокол передачі файлів FTAM, протокол емуляції терміналів VTP.

Стек протоколів TCP/IP. Міжмережні протоколи DARPA. Міжшлюзові протоколи. Формат заголовка TCP. Класи мереж. Доступ до середовища. Маршрутизація Internet, протокол ICMP, UDP, FTP, SNMP, NFS, XDP, RPC, SMTP.

Застосування супутникових і мережних технологій. Супутникові сервіси. Устаткування абонентських станцій супутникового доступу. Налаштування устаткування і програмного забезпечення. Устаткування для проведення відеоконференцій.

*Література* [1; 3–10; 12–15; 17; 18; 23; 25; 29; 32–36; 38]

## **Змістовий модуль II. Менеджмент інформаційної безпеки**

### ***Тема 3. Мережні операційні системи***

Еволюція операційних систем. Концепції мережних операційних систем. Управління ресурсами мережі операційними системами, їх класифікація, особливості побудови, платформи, області використання. Управління процесами в мережах за допомогою ОС: Unix, NetWare, OS-2, Windows. Файлові системи Unix, структура NetWare.

*Література* [1; 3–7; 10; 12; 14; 18; 29; 34; 35; 38; 39]

### ***Тема 4. Захист мереж***

Побудова моделі захисту системи, визначення затрат часу ресурсів та засобів.

Мережні екрани. Брандмауер Windows.

Засіб протоколювання процесів Syslog. Стійкість паролів проти взлому, програма Crack. Файл паролів /etc/passwd. Програма демон (daemon), яка виконує прослуховування повідомлень відповідної служби. Захист режимів Telnet, FTP, Network File System, протоколу POP, агента передачі повідомлень Sendmail, сервера HTTP.

Система пошуку та захисту від вторгнення LIDS (Linux Intrusion Detection/Defence System). Заборона та обмеження доступу до файлів, пам'яті, системам комп'ютера, мережних інтерфейсів, програм, що працюють, вбудованого детектора сканування портів та ін.

Призначення та формати файлів LIDS. cap, LIDS. net, LIDS. pw, LIDS. conf, \$PGDATA/passwd, /etc/services. Вибір паролів та прав

доступу до системи. Багаторівнева аутентифікація. Утиліти Crack5.0 та John The Ripper. Механізм доступу до інформації – програмні закладки. Програма Crack.

Механізм захисту в Linux типу “маскарадинг”. Перекомпіляція ядра для включення захисту типу “маскарадинг”. Система OpenSSH, яка шифрує весь трафік (включаючи паролі).

Створення дерева каталогів із правами доступу. Зміна змісту каталогу access.conf. Додавання користувача та встановлення його прав. Служби, які можуть захищати від кібероблав: Anonymizer.comparison, Компанія Zero-Knowledge Systems, Secure Sockets Layer, Pretty Good Privac

*Література* [2; 11; 16; 19–22; 24; 26; 28; 31; 34; 37; 40]

### **ЗАВДАННЯ ДЛЯ КОНТРОЛЬНИХ РОБІТ**

Контрольна робота є складовою вивчення дисципліни.

Завдання для контрольних робіт підготовлені відповідно до курсу: “Інформаційні мережі” для магістрів.

Мета – допомогти студентам засвоїти теоретичні знання, розвинути і вдосконалити навички, необхідні для виконання професійних функцій зі створення та використання комп’ютерних мереж, програмних та апаратних засобів.

Орієнтовну структуру контрольної роботи і її обсяги наведено в таблиці.

План (розділи)	Обсяг (у сторінках)	Короткий зміст (що потрібно висвітлити)
Вступ	До 1	Мета, загальна характеристика, визначення номера варіанта завдання
Назва кожного питання відповідно до реферату	1-2, загальний обсяг роботи у межах 20–30	Викладення суті питання з приведенням прикладів та посилань на літературні джерела
Висновки	До 1	Прикладне значення
Список літератури	До 1	
Додатки	До 3	Якщо потрібно за змістом



Загальний обсяг роботи не повинен перевищувати 20–30 сторінок машинописного тексту, надрукованого через 2 інтервали, рукописне викладення тексту не повинно перевищувати 18–24 сторінок шкільного зошита.

Виконання та оформлення реферату вимагає від студента розкриття історичних посилок даної проблеми, відповіді на всі питання як теоретичного плану, так і опису технології розв'язання практичної задачі, якщо такі передбачені рефератом.

Відповіді на теоретичні питання потребують ретельної роботи з літературою. Крім виписок і конспектування з літературних джерел, наприклад, із Internet, студент повинен зробити висновки. Робота має виконуватися самостійно. У тексті реферату потрібно давати посилення на використану літературу. Загалом у висновках реферату розглядають питання економічної доцільності і практичного застосування сучасних інформаційних технологій та обчислювальної техніки в інформаційних мережах.

Реферат слід оформляти на стандартних аркушах паперу, зброшурованих у папку. Усі аркуші мають бути пронумеровані. На титульній сторінці потрібно вказати назву вищого навчального закладу, факультет, спеціальність, дисципліну, курс, групу, а також прізвище, ініціали та номер залікової книжки.

На першій сторінці мають бути представлені розрахунок варіанта контрольної роботи та питання варіанта і проставлені номери сторінок, на яких викладено цей матеріал. На останній сторінці студент підписує роботу і ставить дату. Наприкінці роботи подається використана література. Зшити папка повинна бути вложена в поліетиленовий файл та містити дискету з повним текстом, графікою і т. ін. набраного варіанта реферату.

Вибір варіанта контрольної роботи. Кожний студент отримує окреме завдання для виконання КР згідно з варіантом  $Z$ , який обчислюється за формулою:

$$Z = \text{mod}_{17}(NZK + PR - 2000) + 1,$$

де  $NZK$  – номер залікової книжки (студентського квитка) студента;  $PR$  – поточний рік отримання завдання.

Наприклад,  $NZK = 398$ ,  $PR = 2008$ , тоді  $Z = \text{mod}_{17}(398 + 2008 - 2000) + 1 = \text{mod}_{17}(406) + 1 = 15 + 1 = 16$ .

Отже,  $Z = 16$ .

*Зауваження:*

1. Обчислення варіанта має містити у вступі до контрольної роботи.
2. Для довідки:  $\text{mod}_a b$  дорівнює залишку від ділення  $b$  на  $a$ .

*Увага!*

Неправильно оформлена робота повертається без перевірки на дооформлення. Робота, виконана не за своїм варіантом, підлягає переробці.

### **Варіант 1**

1. Асинхронний режим передачі даних — ATM (Asynchronous Transfer Mode).
2. Алгоритм Source-Route Bridging (SRB).
3. Протоколи управління каналами зв'язку PPP (LCP), Synchronous Data-Link Control, HDLC, LAP, LAPB, Logical Link Control, CCITT Recommendation X.25, Frame Relay, SMDS, DQDB, SIP, DNA, XNS, IPX, CMIP, XNS.
4. Призначення Windows NT Server.
5. Комплексний пошук можливих методів доступу.
6. Служби, які можуть захищати від кібероблави: Anonymizer, comparison, Компанія Zero-Knowledge Systems, Secure Sockets Layer, Pretty Good Privac

### **Варіант 2**

1. Вимоги до мереж.
2. Петлі, алгоритм зв'язуючого дерева.
3. Коротка характеристика операційної системи NETWARE.
4. Основи технології, технічні умови, фізичне з'єднання, комутація та інкапсуляція, типи трафіка, формати блока даних, особливості стійкості мережі, послуги, рівні FDDI, UltraNet, ISDN.
5. Зміна змісту каталогу access. conf. Додавлення користувача та встановлення його прав.
6. Огляд найпоширеніших методів “злому”.

### **Варіант 3**

1. Вимоги до устаткування, на якому працюють різні типи операційних систем.
2. Маски для стандартних класів локальних мереж.

3. Особливості операційної системи NETBIOS.
4. Типи адресів: фізичний (MAC-адрес), мережний (IP-адрес) і символний (DNS-ім'я).
5. Термінали захищеної інформаційної системи.
6. Механізм захисту в Linux типу "маскарадінг". Перекомпіляція ядра для включення захисту типу "маскарадінг".

#### **Варіант 4**

1. Гетерогенність та інтегрованість великих комп'ютерних мереж.
2. Коротка характеристика мереж LANTASTIC.
3. Міжмережні протоколи DARPA.
4. Сегменти TCP.
5. Соціальна психологія та інші способи отримання паролів.
6. Механізм доступу до інформації – програмні закладки. Програма Crack.

#### **Варіант 5**

1. Еволюція операційних систем.
2. Архітектура управління мережею ISO.
3. Концентратори, мережні процесори, адаптери каналів зв'язку.
4. Операційна система Linux.
5. Проблеми захисту інформації в Internet та Інтранет.
6. Багаторівнева аутентифікація. Утиліти Crack5.0 та John The Ripper.

#### **Варіант 6**

1. Історія та перспективи стека TCP/IP.
2. Максимальна довжина сегмента та кількість вузлів на ньому.
3. Протокол маршрутизації DECnet Phase IV, IS-IS, RIP, протокол з'єднання PPP, протокол передачі файлів FTAM, протокол емуляції терміналів VTP.
4. Поняття колізії у мережах.
5. Застосування супутникових і мережних технологій.
6. Призначення та формати файлів LIDS. cap, LIDS. net, LIDS. pw, LIDS. conf, \$PGDATA/passwd, /etc/services. Вибір паролів та прав доступу до системи.

#### **Варіант 7**

1. Організації, які займаються стандартизацією мереж.

2. Міжшлюзові протоколи.
3. Управління конфігурацією, ресурсами, захистом даних.
4. Операційні системи в локальних мережах.
5. Управління процесами в мережах за допомогою ОС Unix.
6. Заборона та обмеження доступу до файлів, пам'яті, систем комп'ютера, мережевих інтерфейсів, програм, що працюють, вбудованого детектора сканування портів і т. ін.

### **Варіант 8**

1. Еталонна модель Open Systems Interconnections (OSI) та її рівні.
2. Фізичне підключення, формати блоків, передача маркера. Пріоритети, управління несправностями.
3. Технологія оптоволоконних систем. Електронні компоненти.
4. Особливості та порівняльні характеристики віртуальних мереж.
5. Рівні захисту інформації у мережах.
6. Система пошуку та захисту від вторгнення LIDS (Linux Intrusion Detection/Defence System).

### **Варіант 9**

1. Ієрархічний зв'язок. Формати інформації. Проблеми сумісності. Адресація, блоки даних, пакети.
2. Мережі відділів та робочих груп у корпоративних мережах.
3. Мережі Relkom та FidoNet.
4. Структура стека TCP/IP.
5. Отримання пароля на основі помилок у реалізації.
6. Захист режимів Telnet, FTP, Network File System, протоколу POP, агента передачі повідомлень Sendmail, сервера HTTP.

### **Варіант 10**

1. Визначення маршруту та компоненти маршрутизації.
2. Мережний рівень і модель OSI.
3. Fiber Distributed Data Interface.
4. Сегментація мереж.
5. Брандмауери, мережний екран PIX Firewall, Cisco PIX, FireWall/Plus – фірми NETWORK-1.
6. Файл паролів /etc/passwd. Програма – демон (daemon), яка виконує прослуховування повідомлень відповідної служби.

### **Варіант 11**

1. Типи і метрики алгоритмів маршрутизації та комутації.
2. Порівняння устроїв для об'єднання мереж. Основи технології об'єднання мереж.
3. Операційні системи UNIX.
4. Системи Інтранет та задачі, які вони вирішують.
5. Технологія “клієнт-сервер” у мережі Інтернет.
6. Стійкість паролів проти взлому, програма Crack.

### **Варіант 12**

1. Типи мостів. Прозоре та трансляційне об'єднання мереж за допомогою мостів.
2. Стек протоколів TCP/IP.
3. Структура NetWare.
4. Фізичний, каналний рівень передачі даних у OSI.
5. Монітор безпеки та його основні показники: ізольованість, повнота контролю, верифікованість.
6. Порядок встановлення, зняття паролю облікового запису користувача.

### **Варіант 13**

1. Класи мереж. Доступ до середовища.
2. Файлові системи Unix.
3. Порівняння мереж Ethernet, TELENET, TYMNET, Token Ring та IEEE 802.3, LocalTalk.
4. Маршрутизація Internet, протокол ICMP, UDP, FTP, SNMP, NFS, XDP, RPC, SMTP.
5. Технологія Gigabit Ethernet.
6. Засіб протоколювання процесів Syslog.

### **Варіант 14**

1. Управління протоколами. Керування доступом до мережних ресурсів у мережах Windows for Workgroups.
2. Основні характеристики великої мережі з топологією типу “зірка”.
3. Основні типи кабелів, які застосовуються в локальних мережах.
4. Основні показники локальних мереж на кабелях різних типів.
5. Комплексний пошук можливих методів доступу.

6. Побудова моделі захисту системи, визначення затрат часу, ресурсів та засобів.

### **Варіант 15**

1. Комплекс технічних та програмних засобів захисту інформації.
2. Коротка характеристика мереж NETWARE.
3. Мережі кампусів у корпоративних мережах.
4. Мережевий, транспортний та сеансовий рівень передачі даних у OSI.
5. Метод доступу до середовища передачі CSMA/CD.
6. Методи розширення смуги (середньої швидкості передачі інформації), доступної кожному користувачеві мережі.

### **Варіант 16**

1. Призначення комп'ютерних мереж та їх основні типи.
2. Налаштування параметрів мереж Windows for Workgroups.
3. Об'єднання транспортних потоків окремих мереж у корпоративних мережах.
4. Програмне забезпечення, корпоративна та глобальна адресація, маршрутизація та її рівні.
5. Протоколи доставки дейтаграм DDP, протокол підтримки маршрутної таблиці RTMP, протокол транзакцій ATP, протокол потоку даних ADSP.
6. Призначення прав адміністратора, користувача, гостя.

### **Варіант 17**

1. Призначення, характеристика брандмауерів, комутаторів.
2. Призначення, характеристика маршрутизаторів, шлюзів, концентраторів і мостів.
3. Структура мережної операційної системи.
4. Технологія Fast Ethernet.
5. Управління процесами в мережах за допомогою ОС NetWare.
6. Управління процесами в мережах за допомогою ОС Windows.

### ***ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ***

1. Асинхронний режим передачі даних — ATM (Asynchronous Transfer Mode).
2. Вимоги до мереж.

3. Вимоги до устаткування, на якому працюють різні типи операційних систем.
4. Гетерогенність та інтегрованість великих комп'ютерних мереж.
5. Еволюція операційних систем.
6. Історія та перспективи стека TCP/IP.
7. Застосування супутникових і мережних технологій.
8. Супутникові сервіси.
9. Устаткування абонентських станцій супутникового доступу.
10. Налаштування устаткування і програмного забезпечення.
11. Устаткування для проведення відеоконференцій.
12. Організації, які займаються стандартизацією мереж.
13. Еталонна модель Open Systems Interconnections (OSI) та її рівні.
14. Ієрархічний зв'язок. Формати інформації. Проблеми сумісності. Адресація, блоки даних, пакети.
15. Визначення маршруту та компоненти маршрутизації.
16. Типи і метрики алгоритмів маршрутизації та комутації.
17. Порівняння устроїв для об'єднання мереж. Основи технології об'єднання мереж.
18. Типи мостів. Прозоре та трансляційне об'єднання мереж за допомогою мостів.
19. Петлі, алгоритм зв'язуючого дерева.
20. Алгоритм Source-Route Bridging (SRB).
21. Архітектура управління мережею ISO.
22. Управління конфігурацією, ресурсами, захистом даних.
23. Порівняння мереж Ethernet, TELENET, TYMNET, Token Ring та IEEE 802.3, LocalTalk.
24. Фізичне підключення, формати блоків, передача маркера. Пріоритети, управління несправностями.
25. Розрахунок Ethernet та FastEthernet мереж. Управління протоколами.
26. Керування доступом до мережних ресурсів у мережах Windows for Workgroups.
27. Комплекс технічних та програмних засобів захисту інформації.
28. Коротка характеристика мереж LANTASTIC.
29. Коротка характеристика мереж NETWARE.
30. Коротка характеристика операційної системи NETWARE.
31. Локальні та мережні ресурси.

32. Максимальна довжина сегмента та кількість вузлів на сегменті.
33. Маски для стандартних класів локальних мереж.
34. Мережений рівень і модель OSI.
35. Мережі відділів та робочих груп у корпоративних мережах.
36. Мережі кампусів у корпоративних мережах.
37. Мережі Relkom та FidoNet.
38. Мережний, транспортний та сеансовий рівень передачі даних у OSI.
39. Метод доступу до середовища передачі CSMA/CD.
40. Методи розширення смуги (середньої швидкості передачі інформації), доступної кожному користувачеві мережі.
41. Настроювання параметрів мереж Windows for Workgroups.
42. Об'єднання транспортних потоків окремих мереж у корпоративних мережах.
43. Основи технології, технічні умови, фізичне з'єднання, комутація та інкапсуляція, типи трафіка, формати блока даних, особливості стійкості мережі, послуги, рівні FDDI, UltraNet, ISDN.
44. Концентратори, мережеві процесори, адаптери каналів зв'язку.
45. Програмне забезпечення, корпоративна та глобальна адресація, маршрутизація та її рівні.
46. Технологія оптоволоконних систем. Електронні компоненти.
47. Fiber Distributed Data Interface.
48. Протоколи управління каналами зв'язку PPP (LCP), Synchronous Data-Link Control, HDLC, LAP, LAPB, Logical Link Control, CCITT Recommendation X.25, Frame Relay, SMDS, DQDB, SIP, DNA, XNS, IPX, CMIP, XNS.
49. Протоколи доставки дейтаграм DDP, протокол підтримки маршрутної таблиці RTMP, протокол трансакцій ATP, протокол потоку даних ADSP.
50. Протокол маршрутизації DECnet Phase IV, IS-IS, RIP, протокол з'єднання PPP, протокол передачі файлів FTAM, протокол емуляції терміналів VTP.
51. Стек протоколів TCP/IP.
52. Міжмережні протоколи DARPA.
53. Міжшлюзові протоколи.
54. Класи мереж. Доступ до середовища.
55. Маршрутизація Internet, протокол ICMP, UDP, FTP, SNMP, NFS, XDP, RPC, SMTP.



56. Операційна система Linux.
57. Операційні системи UNIX.
58. Операційні системи в локальних мережах.
59. Основні показники локальних мереж на кабелях різних типів.
60. Основні типи кабелів, які використовуються в локальних мережах.
61. Основні характеристики великої мережі з топологією типу “зірка”.
62. Особливості операційної системи NETBIOS.
63. Особливості та порівняльні характеристики віртуальних мереж.
64. Передумови створення, коротка характеристика великої мережі з топологією типу “зірка”.
65. Поняття колізії у мережах.
66. Призначення Windows NT Server.
67. Призначення комп’ютерних мереж та їх основні типи.
68. Призначення прав адміністратора, користувача, гостя.
69. Призначення, характеристика брандмауерів, комутаторів.
70. Призначення, характеристика маршрутизаторів, шлюзів, концентраторів і мостів.
71. Проблеми захисту інформації в Internet та Інтранет.
72. Реальні (real network), штучні мережі.
73. Реальні та штучні локальні мережі.
74. Рівні захисту інформації у мережах.
75. Сегментація мереж.
76. Сегменти TCP.
77. Системи Інтранет та задачі, які вони вирішують.
78. Структура NetWare.
79. Структура мережної операційної системи.
80. Структура стека TCP/IP.
81. Технологія Gigabit Ethernet.
82. Технологія “клієнт-сервер” у мережі Інтернет.
83. Технологія Fast Ethernet.
84. Типи адреси: фізичний (MAC-адрес), мережевий (IP-адрес) і символічний (DNS-ім’я).
85. Управління процесами в мережах за допомогою ОС NetWare.
86. Управління процесами в мережах за допомогою ОС Unix.
87. Управління процесами в мережах за допомогою ОС Windows.

88. Управління ресурсами мережі операційними системами, їх класифікація, особливості побудови, платформи, області використання.
89. Файлові системи Unix.
90. Захист мереж.
91. Фізичний, каналний рівень передачі даних в OSI.
92. Функції мережних адаптерів, їх основні типи.
93. Сучасна ситуація в галузі інформаційної безпеки.
94. Відповідальність за протиправні дії згідно з законодавством України.
95. Огляд найпоширеніших методів "взлому".
96. Комплексний пошук можливих методів доступу.
97. Термінали захищеної інформаційної системи.
98. Отримання пароля на основі помилок адміністратора й користувачів.
99. Отримання пароля на основі помилок у реалізації.
100. Соціальна психологія та інші способи отримання паролів.
101. Монітор безпеки та його основні показники: ізольованість, повнота контролю, верифікованість.
102. Канали витоку інформації.
103. Порядок встановлення, зняття паролю облікового запису користувача.
104. Брандмауери, Мережний екран PIX Firewall, Cisco PIX, FireWall/Plus — фірми NETWORK-1.
105. Побудова моделі захисту системи, визначення затрат часу ресурсів та засобів.
106. Засіб протоколювання процесів Syslog.
107. Стійкість паролів проти взлому, програма Crack.
108. Файл паролів /etc/passwd. Програма — демон (daemon), яка виконує прослуховування повідомлень відповідної служби.
109. Захист режимів Telnet, FTP, Network File System, протоколу POP, агента передачі повідомлень Sendmail, сервера HTTP.
110. Система пошуку та захисту від вторгнення LIDS (Linux Intrusion Detection/Defence System).
111. Заборона та обмеження доступу до файлів, пам'яті, систем комп'ютера, мережних інтерфейсів, програм, що працюють, вбудованого детектора сканування портів і т. ін.

112. Призначення та формати файлів LIDS. cap, LIDS. net, LIDS. pw, LIDS. conf, \$PGDATA/passwd, /etc/services. Вибір паролів та прав доступу до системи.
113. Багаторівнева аутентифікація. Утиліти Crack5.0 та John The Ripper.
114. Механізм доступу до інформації – програмні закладки. Програма Crack.
115. Механізм захисту в Linux типу “маскарадінг”. Перекомпіляція ядра для включення захисту типу “маскарадінг”.
116. Зміна змісту каталогу access. conf. Додавання користувача та встановлення його прав.
117. Служби, які можуть захищати від кібероблав: Anonymizer. comparison, Компанія Zero-Knowledge Systems, Secure Sockets Layer, Pretty Good Privac.

## **СПИСОК ЛІТЕРАТУРИ**

### *Основна*

1. Буров Э. Комп’ютерні мережі. – Л., 2003. – 584 с.
2. Конев И., Беляев А. Информационная безопасность предприятия. – СПб.: БХВ Петербург, 2003. – 752 с.
3. Кульгин М. В. Компьютерные сети. Практика построения. Для профессионалов. – СПб.: Питер, 2003. – 462 с.
4. Михаил Гук. Аппаратные средства локальных сетей. – СПб.: Питер, 2001. – 572 с.
5. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, прогнозы. – СПб.: Питер, 2003. – 863 с.
6. Введение в сети: Учеб. пособие / Сост. Д. К. Морозов. – Ярославль, 1995.
7. Хазер Остерлех. IP маршрутизация. – К.: Диасофт, 2002. – 537 с.

### *Додаткова*

8. Волоконно-оптические линии связи: Справочник / Под ред. С. В. Свечникова и Л. М. Андрушко. – К.: Техника, 1988.
9. Волоконно-оптические системы передачи и кабели: Справочник / Под ред. И. И. Гроднева, А. Г. Мурадяна, Р. М. Шарафутдинова и др. – М.: Радио и связь, 1993.

10. *Netware* Версия 3.12. Концепции.-Novell Inc. / Пер. с англ. НПО Информатика. — Иваново: Novell Inc., 1994.
11. *Баранов А. П., Зегжда Д. П., Зегжда П. Д.* и др. Теоретические основы информационной безопасности (Дополнительные главы): Учеб. пособие. — СПб., 1998. — 173 с.
12. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Питер, 2001. — 668 с.
13. *Бройдо В. Л.* Вычислительные системы, сети и телекоммуникации: Учеб. для вузов. — СПб., 2002. — 630 с.
14. *Девис Д. и др.* Вычислительные сети и сетевые протоколы. — М.: Мир, 1982. — 563 с.
15. *Дейв Молта.* Удаленный доступ по TCP // IP Network Computing. 1995. — 15 груд. — С. 112.
16. *Домарев В. В.* Безопасность информационных технологий. — СПб.: DiaSoft, 2002. — 688 с.
17. *Дуг Лоу.* Компьютерные сети для “чайников”. — К.: Диалектика, 1995.
18. *Дьяконов В. П.* Internet: Настольная книга пользователя. — М.: Молот-Р., 1999. — 573 с.
19. *Защита* компьютерных систем от разрушающих программных воздействий: Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 128 с.
20. *Защита* программного обеспечения: Пер. с англ. / Д. Гроувер, Р. Сатер, Дж. Фипс и др.; За ред. Д. Гроувера. — М.: Мир, 1992. — 285 с.
21. *Зегжда Д. П., Калинин М. О., Степанов П. Г.* Теоретические основы информационной безопасности. Защищенные операционные системы: Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 69 с.
22. *Зегжда Д. П., Корт С. С., Каулио В. В.* Теоретические основы информационной безопасности: Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 34 с.
23. *Карпенко С., Шишигин И.* Internet в вопросах и ответах. — СПб.: ВHV, 1997.
24. *Касперский Е.* “Дыры” в MS-DOS и программы защиты информации // КомпьютерПресс. — 1991. — № 10.
25. *Козелев А. И.* Анализ состояния и перспектив развития цифровых сетей связи на основе наземных и подводных волоконно-

- оптических систем передачи с учетом строительства ТСЛ // Зарубежная радиоэлектроника. — 1993.
26. *Краснов А. В.* Некоторые проблемы безопасности в сетях ЭВМ и способы их решения // Защита информации. — 1992. — № 3–4.
  27. *Медведовский И. Д., Безгачев В. А., Гореленков А. П.* Информационная безопасность распределенных вычислительных систем: Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 73 с.
  28. *Методы и средства защиты информации* / За ред. Ю. С. Ковтунюка. — К.: ЮНИОР, 2003. — 501 с.
  29. *Олаф Курч.* Руководство администратора сети в ОС Linux. 1992–1994. <http://ttc.ryazan.ru/archive/nag.htm>
  30. *Перри П. Дж.* Секреты World Wide Web. — К.: Диалектика, 1997.
  31. *Перший А. Ю.* Организация защиты вычислительных систем // КомпьютерПресс. — 1992. — № 10–11. — С. 35–50.
  32. *Солоницын Ю., Холмогоров В.* Энциклопедия. Интернет. — СПб., 2002. — 592 с.
  33. *Стэн Шатт.* Мир компьютерных сетей: Пер. с англ. — К.: BHV, 1996. — 288 с.
  34. *Немет Е., Снайдер Г., Сибас С. и др.* UNIX: Руководство системного администратора. — К.: BHV, 1997. — 830 с.
  35. *Хазер Остерлех.* TCP/IP. Семейство протоколов передачи данных в сетях компьютеров. — К.: Диасофт, 2002. — 567 с.
  36. *Хонникатт, Джерри.* Использование Internet. — К.; М.; СПб.: Издат. дом “Вильямс”, 1998. — 272 с.
  37. *Хорев А. А.* Способы и средства защиты информации. — М.: МО РФ, 1998. — 316 с.
  38. *Якубайтис Э. А.* Архитектура вычислительных сетей. — М.: Статистика, 1980. — 277 с.
  39. *Якубайтис Э. А.* Локальные информационно-вычислительные сети. — Рига: Зинатне, 1985. — 284 с.
  40. *Ярочкин В. И.* Безопасность информационных систем. — М.: Ось-89, 1996.

## ***ЗМІСТ***

Пояснювальна записка .....	3
Тематичний план дисципліни “Інформаційні мережі”.....	5
Зміст дисципліни “Інформаційні мережі” .....	6
Завдання для контрольних робіт.....	8
Питання для самоконтролю .....	14
Список літератури.....	19



Відповідальний за випуск *А. Д. Вегеренко*  
Редактор *Т. М. Коліна*  
Комп'ютерне верстання *Т. Г. Замура*

**МАУП**

Зам. № ВКЦ-3627

Міжрегіональна Академія управління персоналом (МАУП)  
03039 Київ-39, вул. Фрометівська, 2, МАУП