МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

НАВЧАЛЬНА ПРОГРАМА
дисципліни

“ІНФОРМАЦІЙНА БЕЗПЕКА”
(для магістрів)

Київ 2006

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

Затверджено на засіданні кафедри інформатики та інформаційних технологій (протокол № 21 від 03.02.06)

Схвалено Вченою радою Міжрегіональної Академії управління персоналом

Ахрамович В. М. Навчальна програма дисципліни "Інформаційна безпека" (для магістрів). — К.: МАУП, 2006. — 26 с.

Навчальна програма містить пояснювальну записку, тематичний план, зміст дисципліни "Інформаційна безпека", вказівки до виконання контрольної роботи, варіанти контрольних робіт, питання для самоконтролю, а також список літератури.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Останнім часом повідомлення про атаки на інформацію, про хакерів і комп'ютерні зломи заполонили всі засоби масової інформації. З масовим упровадженням комп'ютерів у всі сфери діяльності людини обсяг інформації, що зберігається в електронному вигляді, збільшився в тисячі разів. І тепер скопіювати за півхвилини і понести дискету, флеш-пам'ять із файлом (лами), що містить план випуску продукції, набагато простіше, ніж копіювати або переписувати купу паперів. А з появою комп'ютерних мереж навіть відсутність фізичного доступу до комп'ютера перестала бути гарантією збереження інформації.

При вирішенні багатьох завдань із прикладної сфери діяльності людини майбутній спеціаліст-менеджер стикається із проблемою захисту інформації, програмних продуктів, технічного забезпечення АРМ фахівців, комп'ютерних мереж, інформаційних систем. Для спеціалістів істотного значення набуло вміння не тільки застосовувати сучасні комп'ютерні програми, інформаційні технології, а й захищати інформацію, програмні пристрої, комп'ютерні мережі та їх складові.

Сучасні програмні продукти, інформаційні системи й технології базуються на апаратних і програмних засобах. Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, інших фінансових установ призводить до порушення нормального функціонування підприємств, значних фінансових збитків, а інколи до повного їх банкрутства.

Мета вивчення дисципліни "Інформаційна безпека"

1. Оволодіння студентами комплексом знань в області захисту інформації, системами й методами визначення захищеності програмних продуктів, пристроїв; комп'ютерних мереж, їх складових та набуття на основі цих знань практичних навичок і теоретичних знань, необхідних для творчого підходу в питанні сучасного та в майбутньому оперативного захисту комп'ютерної техніки й інформації.
2. Оволодіння студентами алгоритмами створення сучасних програм захисту; алгоритмами кодування; сучасними методами, технологією; комп'ютерними програмними, технічними засоба-

ми в області захисту: операційних систем, текстових редакторів, табличних процесорів, систем управління базами даних, конфіденціальної інформації і т. п. Набуття на основі вказаних знань практичних навичок, необхідних для розробки систем захисту, керування розробкою систем захисту, а на основі вказаного, нормального забезпечення роботи фінансових організацій, регіонів країни зі збереженням характеристик трафіку, швидкості санкціонованого доступу і т. п.

3. Оволодіння концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденціальних документів; стратегією вибору систем виявлення атак, навичками роботи з пристроями безпеки в локальних і глобальних комп'ютерних мережах з метою використання їх, можливостей для покращення показників безпеки в них.

Завдання дисципліни

У результаті вивчення дисципліни студенти повинні:

- знати про джерела і способи дії загроз на об'єкти інформаційної безпеки установ, про правові і нормативні акти, які визначають систему захисту інформації в державі; про документи, що визначають ступінь захищеності комп'ютерних систем; методи аналізу надійності системи захисту інформації в комп'ютерних системах; основні методи, технологію, принципи і правила захисту електронних обчислювальних машин, у тому числі персональних комп'ютерів, їх елементів і об'єктів комп'ютерних мереж;
- мати достатньо повне уявлення про алгоритми створення сучасних програм, алгоритми кодування та застосування стандартного програмного забезпечення захисту; методи і технологію захисту операційних систем, текстових редакторів, табличних процесорів, системи управління базами даних у локальних, корпоративних і глобальних комп'ютерних мережах банків та інших фінансових установ, на основі вивчених алгоритмів вміти розробляти нові програмні складові захисту в майбутньому;
- набути практичних навичок роботи з концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденціальних документів; роботи із системами й методами визначення захищеності носіїв інформації; створення засобами стандартного програмного забезпечення елементів захисту ін-

формації; формулювати завдання з питань захисту інформації, та формалізуючи їх, визначати шляхи їх вирішення.

Місце дисципліни та її значення в навчальному процесі

Із задоволенням суспільних потреб виникають проблеми інформаційного забезпечення всіх сфер діяльності людини. Одна з них — забезпечення надійного захисту інформації. Особливої гостроти вона набуває у зв'язку з масовою комп'ютеризацією всіх видів діяльності людини, при об'єднанні ЕОМ у комп'ютерні мережі та підключення до Інтернету. Вибір серед більшості сучасних методів та засобів захисту таких, що найбільше відповідають конкретним умовам діяльності та забезпечують достатній рівень безпеки, є досить складним завданням, особливо для початківців. Разом з тим, багато технологій мають чимало спільних рис, як щодо розробки, так і використання. Це дає можливість вивчати сучасні технології на прикладах, які незважаючи на новизну, вже стали класичними. Наприклад: засоби захисту операційної системи, мережеві екрани, криптографічні системи, системи визначення атак і реакцій на атаку, системи моніторингу інформаційної безпеки. При цьому вивчення цих технологій передбачає ґрунтовну теоретичну базу та аналіз вітчизняних і зарубіжних нормативних документів у галузі захисту інформації. Для кращого розуміння технологій захисту передбачено вивчення методики та засобів здійснення атак на комп'ютерні системи та мережі.

Актуальним на сьогодні є підготовка менеджерів, які вміють ефективно організовувати захист інформації в комп'ютерних системах і мережах, володіють сучасними технологіями захисту інформації та мають достатню кваліфікацію для проектування та розробки нових засобів і методів захисту. Саме на підготовку таких спеціалістів розрахована дисципліна "Інформаційна безпека".

Міждисциплінарні зв'язки. Ця дисципліна ґрунтується на знаннях з курсів "Інформатика та комп'ютерна техніка", "Методи прийняття управлінських рішень", "Системи технологій", "Організація діяльності фірми", "Підприємницьке право"та інші і сприятиме кращому розумінню предмета при вивченні подальших навчальних дисциплін: "Основи зовнішньоекономічної діяльності", "Міжнародні економічні відносини", "Податкова система" тощо.

Передбачені форми контролю знань

Під час вивчення курсу передбачається систематична практична робота студентів за комп'ютерами, в тому числі у мережах як під керівництвом викладача, так і самостійно, а також постійний контроль у процесі вивчення дисципліни (захист лабораторних робіт, опитування на лекціях) і періодичний контроль (контроль знань за кожним модулем, періодичні тестування, залік).

ТЕМАТИЧНИЙ ПЛАН
дисципліни
"ІНФОРМАЦІЙНА БЕЗПЕКА"

№ пор.	Назва змістових модулів і тем
1 2	**Змістовий модуль 1. Менеджмент інформаційної безпеки** Інформаційна безпека Безпека інформації за допомогою апаратних засобів
3	**Змістовий модуль 2. Менеджмент безпеки інформаційних систем** Безпека комп'ютерних мереж
Разом	годин: 54

ЗМІСТ
дисципліни
"ІНФОРМАЦІЙНА БЕЗПЕКА"

Змістовий модуль 1. Менеджмент інформаційної безпеки

Тема 1. Інформаційна безпека

Категорії інформаційної безпеки щодо інформації та інформаційних систем.

Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж. Незаконні дії з документами на переказ, платіжними картками та іншими засобами

доступу до банківських рахунків, інших фінансових установ, обладнанням для їх виготовлення.

Відповідальність за протиправні дії згідно із законодавством України.

Сучасна ситуація у сфері інформаційної безпеки. Категорії інформаційної безпеки. Абстрактні моделі захисту інформації. Огляд найбільш поширених методів "злому". Комплексний пошук можливих методів доступу. Термінали захищеної інформаційної системи. Отримання пароля на основі помилок адміністратора й користувачів. Отримання пароля на основі помилок у реалізації. Соціальна психологія та інші способи отримання паролів.

Класифікація інформаційних об'єктів. Вимоги до роботи з конфіденційною інформацією. Політика ролей. Створення політики інформаційної безпеки. Методи забезпечення безвідмовності.

Ідентифікація й аутентифікація. Механізми підзвітності та аудиту. Монітор безпеки та його основні показники: ізольованість, повнота контролю, верифікованість. Протоколи аутентифікації.

Основні елементи політики безпеки: довільне управління доступом; безпека повторного використання об'єктів; мітки безпеки; примусове управління доступом.

Класи безпеки. Критерії інформаційної безпеки. Канали витоку інформації.

Парольний захист комп'ютера при його запуску. Парольний захист комп'ютера в режимі чекання і сплячки. Захист файлів у режимі чекання (шляхом призначення пароля екранній заставці). Дозвіл іншим користувачам створювати власні настроювання. Зміна мережевого пароля. Запуск Windows у режимі захисту від збоїв. Керування доступом до папок і принтерів.

Послідовність встановлення захисту на файл у Microsoft Word. Типи захисту тексту в Microsoft Word. Послідовність зняття захисту з тексту в Microsoft Word. Послідовність встановлення захисту на комірки, листи та книгу в Microsoft Excel.

Вимоги до паролів у програмі MS Access. Порядок установлення, зняття паролю баз даних. Порядок установлення, зняття пароля облікового запису користувача. Порядок установлення, зняття пароля програми Microsoft Visual Basic для додатків.

Порядок захисту сторінки доступу. Порядок приховування, відображення елементів баз даних.

Класифікація криптоалгоритмів. Тайнопис, криптографія з ключем, симетричні та асиметричні криптоалгоритми. Скремблери. Мережа Фейштеля. Перестановочні, підстановочні криптоалгоритми.

Поточні, блочні шифри. Одиниці кодування.

Шифрування заміною (підстановкою), перестановкою, маршрути Гамільтона, гаміювання, аналітичних перетворень, комбіновані методи.

Порядок шифрування даних за допомогою архіваторів і пошуку паролів. Використання програми Advanced ZIP Password Recovery. Прямий перебір паролів, перебір за маскою, атака за словником. Складові вікна програми Advanced ZIP Password Recovery.

Вимоги до паролів документів Microsoft Office. Складові вікна програми Advanced Office 97 Password Recovery. Режими підбору паролів та їх характеристики. Маски пошуку паролів. Залежність часу пошуку пароля від його параметрів.

Література [1–5; 8–12; 14–18; 20; 23; 24; 28–31; 33; 34; 37–39]

Тема 2. Безпека інформації за допомогою апаратних засобів

Визначення каналів витоків інформації. Їх типи, особливості.

Системи ідентифікації й аутентифікації користувача (традиційні та біометричні параметри). Модуль Internet Log. Системи шифрування дискових даних (системи прозорого і спеціального видів шифрування). Системи шифрування даних, які передаються в мережах (канальне та абонементне шифрування). Системи аутентифікації електронних даних (імітовставка, електронний підпис). Кабінетний замок "Сонет". Система FireWall-1/VPN-1. Система OmniGuard/ Enterprise Security Manager компанії Axent.

Брандмауери. Мережевий екран PIX Firewall, Cisco PIX, FireWall/ Plus — фірми NETWORK-1. Апаратно-програмний комплекс захисту інформації "ШИП", "Dallas Lock". Криптографічний адаптер. Процесор безпеки мережі. Локатори ліній зв'язку. Локатор провідникових ліній "Вектор". Нелінійний радіолокатор NR-900E. Сканер NetRecon. Аналізатор телефоних ліній SP-18/T "Багер-01". Детектор електромагнітного поля Д-006.

Зонд-монітори. Зонд-монітор СРМ-700 (Акула). Вимірювачі частот, нелінійні радіолокатори. Ручний вимірювач частот РИЧ-2. Універсальні комплекси моніторингу. Універсальний комплекс моніторингу технічних каналів витоку інформації "КРОНА-6000".

Система NetRecon. Багатофункціональні комплекси захисту. Комплексний пошуковий прилад ST-31 "Пиранья". Захист приміщень. Система "Полонез", "Менует". Портативний пошуковий прилад Д-008. СВЧ-перетворювач (конвертор) ПС-3900, ПС-5700, ПС-6000. Спектральний корелятор OSC-5000 (OSCOR).

Засоби управління криптографічними ключами: генерація, зберігання і розподілення ключів.

Тестування дисків: компонента Disk Diagnostics Contents, SMARTTests. Partition-Tests, DataAdvisor (Радник Даних), Ontrack JumperViewer, SizeManager, Data Recovery (Відновлення Даних).

Основні кроки відновлення даних: компонента AdvancedRecovery, DeletedRecovery, FormatRecovery. Призначення та особливості програми Disk Wiper. Створення нових логічних дисків, їх форматування, перевірка правильності позначення створеного диску. Послідовність очистки вільного простору на диска, повної очистки диска, видалення логічного диску, приховування диску та його відображення.

Література [1; 4; 5; 13; 18; 21; 22; 26–28; 31–33; 35; 36; 42]

Змістовий модуль 2. Менеджмент безпеки інформаційних систем

Тема 3. Безпека комп'ютерних мереж

Стратегія захисту інформації у фінансово-економічних інформаційних системах. Комплекс технічних і програмних засобів захисту інформації.

Сучасна ситуація у сфері інформаційної безпеки. Рівні мережевих атак (фізичний, канальний, мережевий, транспортний, сеансовий) за моделлю OSI. Типи атак (відмова від обслуговування, перебір варіантів, метод соціального інжинірингу, пасивна атака, атака типу "Sniff'", неправильний адрес мережі, "закидання" пакетами, недозволене з'єднання, недозволений протокол, ICMП атака, несанкціоноване адміністрування, зміна пароля, DNS атака, недозволений час та ін.).

Вимоги при роботі з конфіденціальною інформацією. Політика ролей. Технології цифрових підписів.

Стратегія вибору систем виявлення атак.

Термінали захищеної інформаційної системи. Отримання пароля на основі помилок адміністратора та користувача. Отримання пароля на основі помилок у реалізації. Соціальна психологія та інші спосо-

би отримання пароля. Призначення програми Super File Encryption. Порядок шифрування та дешифрування файлів у програмі Super File Encryption. Порядок підбору параметрів шифрування та дешифрування файлів. Призначення утиліти (T-CEC Pro). Порядок шифрування, дешифрування файлів утилітою (T-CEC Pro). Призначення системи шифрування даних BestCrypt. Короткі характеристики алгоритмів шифрування, які підтримує BestCrypt. Поняття контейнера в системі шифрування даних BestCrypt. Призначення генератора ключів у системі BestCrypt. Особливості роботи зі Схованим і Оригінальним контейнерами.

Визначення комп'ютера, який працює в мережі в режимі "Sniff".

Загальні відомості про блокові шифри. Мережа Фейштеля.

Методи рандомізації повідомлень. Генератори випадкових і псевдовипадкових послідовностей. Алгоритм Хаффмана. Стандарт блокових шифрів AES. Алгоритм RSA. Блоковий шифр TEA. Стандарт DES (Data Encryption Standard). Приклад дешифрування.

Системи виявлення атак, стратегія вибору.

Попередня оцінка конфіденційності та цінності інформації. Планування витрат часу та засобів на несанкціонований доступ до системи, із системним забезпеченням Microsoft Windows і програм пакета Microsoft Office, виділення найбільших загроз (несанкціоноване читання, зміна інформації, її вилучення, знищення тощо).

Побудова моделі захисту системи, визначення витрат часу ресурсів і засобів.

Засіб протоколювання процесів Syslog. Стійкість паролів проти злому, 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, мережевих інтерфейсів, програм, що працюють, встроєного детектора сканування портів і т. д.

Призначення та формати файлів LIDS.cap, LIDS.net, LIDS.pw, L IDS.conf, $PGDATA/passwd, /etc/services. Вибір паролів і 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 “маскарадінг”. Перекомпіляція ядра для включення захисту типу “маскарадінг”. Система OpenSSH, яка шифрує весь трафік (у тому числі паролі).

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

Література [1–8; 10; 19; 21; 25–27; 29; 33; 35–38; 40–42]

ВКАЗІВКИ ДО ВИКОНАННЯ КОНТРОЛЬНОЇ РОБОТИ

Контрольна робота є складовою вивчення дисципліни.

Завдання підготовлені відповідно до курсу “Інформаційна безпека” для магістрів спеціальності “Менеджмент організацій” — студентів заочної форми навчання.

Структура контрольної роботи

Орієнтовна структура і обсяги контрольної роботи:

План (розділи)	Обсяг у сторінках (приблизно)	Короткий зміст (що потрібно висвітлити)
Вступ	Одна	Мета, загальна характеристика, визначення номера варіанта завдання
Назва кожного питання відповідно до завдання	1–4	Викладення суті питання з наведенням прикладів і посилань на літературні джерела
Висновки	Одна	Прикладне значення
Список літератури	Одна	
Додатки	Три	Якщо є

Загальний обсяг роботи — не більше 25 сторінок машинописного тексту, надрукованого через один інтервал.

ВИКОНАННЯ ТА ОФОРМЛЕННЯ КОНТРОЛЬНОЇ РОБОТИ

Студент повинен виконати контрольну роботу, висвітлюючи питання теоретичного плану, а також і описати технологію розв'язання практичної задачі.

Відповіді на теоретичні питання потребують ретельної роботи з літературою. Крім конспектування і виписок з літературних джерел, наприклад із Інтернету, студент повинен зробити висновки. Робота повинна бути виконана самостійно. У тексті контрольної роботи потрібно давати посилання на використану літературу. Відповідь на практичне питання повинна включати організаційно-функціональну сутність задачі, характеристику вихідних і вхідних документів і реквізитів, алгоритм рішення, вибір програмного забезпечення задачі, форми вихідних документів, що отримані в результаті розв'язання задачі. За результатами розв'язання обчислювальної задачі потрібно зробити висновок з питань безпеки.

У загальних висновках висвітлюються питання безпеки і практичного застосування сучасних інформаційних технологій та обчислювальної техніки.

Контрольна робота оформлюється на стандартних аркушах паперу, зброшурованих у папку. Усі сторінки нумерують. На титульній сторінці необхідно вказати назву вищого навчального закладу, факультет, спеціальність, дисципліну, курс, групу, а також прізвище, ініціали та номер залікової книжки.

На першій сторінці повинні бути представлені розрахунок варіанта контрольної роботи та питання варіанта і проставлені номери сторінок, на яких викладено матеріал. На останній сторінці студент підписує роботу і ставить дату. Наприкінці роботи необхідно дати використану літературу. Зшита папка з дискетою з повним текстом, графікою вибраного варіанта контрольної роботи вкладається в поліетиленовий файл.

ВИБІР ВАРІАНТА КОНТРОЛЬНОЇ РОБОТИ

1. Кожний студент отримує окреме завдання для виконання КР згідно з варіантом Z, який обчислюється за залежністю:

$$Z = mod_{18}\,(NZK + PR - 2000) + 1,$$

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

Наприклад, $NZK = 398$, $PR = 005$, тоді

$Z = mod_{20}(398+2005-2000)+1 = mod_{20}(403) + 1 = 3 + 1 = 4.$

Отже, $Z = 4$.

Зауваження. 1. Обчислення варіанта повинно бути у вступі контрольної роботи.

2. Для довідки: $mod_a b$ дорівнює залишку від ділення b на a.

ВАРІАНТИ КОНТРОЛЬНИХ РОБІТ

Варіант 1

1. Три етапи розвитку захисту інформації.
2. Схема простійших дій над числами блоковим криптоалгоритмом. Керування доступом до папок і принтерів в ОС Windows.
3. Призначення програми Super File Encryption.
4. Порядок захисту сторінки доступу у програмі MS Access.

Варіант 2

1. Історія зародження шифрування.
2. Стандарт DES (Data Encryption Standard). ГОСТ 28147-89.
3. Парольний захист комп'ютера при його запуску.
4. Порядок шифрування та дешифрування файлів у програмі Super File Encryption.
5. Як проводиться приховування диска та його відображення у програмі Windows Disk Wiper?

Варіант 3

1. Категорії інформаційної безпеки щодо інформації та інформаційних систем.
2. Огляд найбільш поширених методів "злому".
3. Парольний захист комп'ютера в режимі чекання і сплячки.
4. Призначення генератора ключів у системі BestCrypt.
5. Маски пошуку паролів у програмі Advanced Office 97 Password Recovery.

Варіант 4

1. Класи безпеки.
2. Симетричні криптосистеми.
3. Захист файлів у режимі чекання (шляхом призначення пароля екранній заставці) в ОС Windows.
4. Призначення утиліти (T-CEC Pro).

5. Де зберігаються окремі типи паролів у програмі MS Access? За яким стандартом шифрується пароль у заголовку файла? В якому файлі зберігається інформація про користувачів?

Варіант 5

1. Основні загрози інформаційній безпеці автоматизованої інформаційної системи.
2. Керування ключами у криптографії.
3. Дозвіл іншим користувачам створювати власні настроювання в ОС Windows.
4. Порядок шифрування дешифрування файлів утилітою (T-CEC Pro).
5. Послідовність повної очистки диску в програмі Windows Disk Wiper.

Варіант 5

1. Несанкціонований доступ до інформації.
2. Рівні мережевих атак за моделлю OSI.
3. Як приховати формули в комірках у Microsoft Excel?
4. Короткі характеристики алгоритмів шифрування, які підтримує BestCrypt?
5. Призначення програми Disk Wiper.

Варіант 6

1. Призначення системи шифрування даних BestCrypt.
2. Сучасна ситуація у сфері інформаційної безпеки.
3. Випадкові дії та дії з попереднім наміром щодо безпеки інформаційної системи.
4. Шифрування простою перестановкою.
5. Зміна мережного пароля в ОС Windows.

Варіант 7

1. Рівні забезпечення інформаційної безпеки.
2. Соціальна психологія та інші способи отримання паролів.
3. Мережеві компоненти, що атакуються.
4. Запуск Windows у режимі захисту від збоїв.
5. Послідовність видалення логічного диска у програмі Windows Disk Wiper.

Варіант 8

1. Огляд найбільш поширених методів “злому”.
2. Технічні, програмно-апаратні та адміністративні засоби захисту інформації.
3. Перестановочні, підстановочні криптоалгоритми.
4. Послідовність очистки вільного простору на диску в програмі Windows Disk Wiper.
5. Порядок установлення, зняття пароля програми Microsoft Visual Basic для додатків у програмі MS Access.

Варіант 9

1. Категоризація інформації.
2. Створення політики інформаційної безпеки.
3. Правило Огюста Керкхоффа. Призначення рандомізатора.
4. Захист інформації в Microsoft Word та у Microsoft Excel.
5. Складові діалогового віконця програми Advanced ZIP Password Recovery.

Варіант 10

1. Класифікація інформації за рівнем конфіденційності у США.
2. Криптоаналіз.
3. Категорії інформаційної безпеки.
4. Порядок установлення, зняття пароля баз даних у програмі MS Access.
5. Як перевірити правильність позначення створеного диска у програмі Windows Disk Wiper?

Варіант 11

1. Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем і комп’ютерних мереж. Законодавство України.
2. Криптосистеми з відкритим ключем.
3. Класифікація інформаційних об’єктів щодо захисту інформації.
4. Послідовність встановлення захисту на комірки в Microsoft Excel.
5. Порядок захисту сторінки доступу баз даних у програмі MS Access.

Варіант 12

1. Класи безпеки. Критерії інформаційної безпеки. “Оранжевая книга” США.
2. Абстрактні моделі захисту інформації.
3. Які типи паролів використовуються у програмі MS Access? Вимоги до паролів у програмі MS Access. Порядок приховування, відображення елементів баз даних.
4. Принцип шифрування Цезаря.
5. Як провести форматування створеного диска у програмі Windows Disk Wiper?

Варіант 13

1. Системи аутентифікації електронних даних.
2. Термінали захищеної інформаційної системи.
3. Послідовність встановлення захисту на книгу в Microsoft Excel.
4. Типи захисту тексту в Microsoft Word.
5. Як створити новий логічний диск за допомогою програми Windows Disk Wiper?

Варіант 14

1. Проблема захисту інформації шляхом її перетворення.
2. Абстрактні моделі захисту інформації.
3. Які програмні продукти застосовуються для пошуку паролів?
4. Особливості програми Windows Disk Wiper.
5. Порядок установлення, зняття пароля облікового запису користувача у програмі MS Access.

Варіант 15

1. Потокові шифри. Скремблери. Принцип дії.
2. Отримання пароля на основі помилок у реалізації.
3. Вимоги до паролів документів Microsoft Office.
4. Принцип шифрування Цезаря.
5. Послідовність встановлення захисту на листи в Microsoft Excel.

Варіант 16

1. Дані про порушників доступу до інформації за DataPro Research.
2. Отримання пароля на основі помилок адміністратора й користувачів.

3. Принцип шифрування в давніх іудейських текстах.
4. Порядок установлення, зняття паролю баз даних у програмі MS Access.
5. Залежність часу пошуку пароля від його параметрів у програмі Advanced Office 97 Password Recovery.

Варіант 17

1. Політика ролей.
2. Що означає залежність $K = \max (int(N\,0{,}1\times 3)+1{,}3)$.
3. Блокові шифри.
4. Порядок підбору параметрів шифрування та дешифрування файлів у BestCrypt.
5. Поняття контейнера в системі шифрування даних BestCrypt. Призначення генератора ключів у системі BestCrypt.

Варіант 18

1. Системи електронного підпису.
2. Вимоги по роботі з конфіденційною інформацією.
3. Методи забезпечення безвідмовності сервізів і служб.
4. Особливості роботи зі Схованим і Оригінальним контейнерами в системі BestCrypt.
5. Порядок пошуку паролів в архівах із кількома файлами, які мають різні паролі.

Варіант 19

1. Принцип роботи шифрувального устрою скитала.
2. Два напрями криптології.
3. Особливості програмної криптології.
4. Порядок установлення, зняття паролю облікового запису користувача у програмі MS Access.
5. Складові діалогового віконця програми Advanced Office 97 Password Recovery.

Варіант 20

1. Принцип дешифрування шифру скитала.
2. Особливості апаратної криптології.
3. Поняття криптоаналізу.
4. Загальна схема захищеного зв'язку.

5. Режими підбору паролів та їх характеристики у програмі Advanced Office 97 Password Recovery.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Сучасна ситуація у сфері інформаційної безпеки.
2. Категорії інформаційної безпеки щодо інформації та інформаційних систем.
3. Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж.
4. Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, інших фінансових установ, обладнанням для їх виготовлення.
5. Відповідальність за протиправні дії згідно із законодавством України.
6. Категорії інформаційної безпеки.
7. Абстрактні моделі захисту інформації.
8. Огляд найбільш поширених методів "злому".
9. Комплексний пошук можливих методів доступу.
10. Термінали захищеної інформаційної системи.
11. Отримання пароля на основі помилок адміністратора і користувачів.
12. Отримання пароля на основі помилок у реалізації.
13. Соціальна психологія та інші способи отримання паролів.
14. Класифікація інформаційних об'єктів.
15. Вимоги до роботи з конфіденційною інформацією.
16. Політика ролей.
17. Створення політики інформаційної безпеки.
18. Методи забезпечення безвідмовності.
19. Ідентифікація й аутентифікація.
20. Механізми підзвітності та аудиту.
21. Монітор безпеки та його основні показники: ізольованість, повнота контролю, веріфікованість.
22. Протоколи аутентифікації.
23. Основні елементи політики безпеки: довільне управління доступом; безпека повторного використання об'єктів; мітки безпеки; примусове управління доступом.
24. Класи безпеки. Критерії інформаційної безпеки.
25. Канали просочування інформації.

26. Парольний захист комп'ютера при його запуску. Парольний захист комп'ютера в режимі чекання і сплячки. Захист файлів у режимі чекання (шляхом призначення пароля екранній заставці).
27. Дозвіл іншим користувачам створювати власні настроювання. Зміна мережного пароля.
28. Запуск Windows у режимі захисту від збоїв.
29. Керування доступом до папок і принтерів.
30. Послідовність встановлення захисту на файл у Microsoft Word.
31. Типи захисту тексту в Microsoft Word.
32. Послідовність зняття захисту з тексту в Microsoft Word.
33. Послідовність встановлення захисту на комірки, листи та книгу в Microsoft Excel.
34. Вимоги до паролів у програмі MS Access. Порядок установлення, зняття пароля баз даних.
35. Порядок установлення, зняття пароля облікового запису користувача.
36. Порядок установлення, зняття пароля програми Microsoft Visual Basic для додатків.
37. Порядок захисту сторінки доступу.
38. Порядок приховування, відображення елементів баз даних.
39. Класифікація криптоалгоритмів.
40. Тайнопис, криптографія з ключем, симетричні та асиметричні криптоалгоритми.
41. Скремблери. Мережа Фейштеля.
42. Перестановочні, підстановочні криптоалгоритми.
43. Поточні, блочні шифри. Одиниці кодування.
44. Шифрування заміною (підстановкою), перестановкою, маршрути Гамільтона, гаміювання аналітичних перетворень, комбіновані методи.
45. Порядок шифрування даних за допомогою архіваторів і пошуку паролів.
46. Використання програми Advanced ZIP Password Recovery.
47. Прямий перебір паролів, перебір за маскою, атака за словником. Складові вікна програми Advanced ZIP Password Recovery.
48. Вимоги до паролів документів Microsoft Office.
49. Складові вікна програми Advanced Office 97 Password Recovery.
50. Режими підбору паролів та їх характеристики.

51. Маски пошуку паролів. Залежність часу пошуку пароля від його параметрів.
52. Визначення каналів витоків інформації. Їх типи, особливості.
53. Системи ідентифікації й аутентифікації користувача (традиційні та біометричні параметри).
54. Системи шифрування дискових даних (системи прозорого і спеціального видів шифрування).
55. Системи шифрування даних, які передаються у мережах (канальне та абонементне шифрування).
56. Призначення програми Super File Encryption.
57. Порядок шифрування та дешифрування файлів у програмі Super File Encryption.
58. Порядок підбору параметрів шифрування та дешифрування файлів.
59. Призначення утиліти (T-CEC Pro). Порядок шифрування та дешифрування файлів утилітою (T-CEC Pro).
60. Призначення системи шифрування даних BestCrypt.
61. Короткі характеристики алгоритмів шифрування, які підтримує BestCrypt.
62. Поняття контейнера в системі шифрування даних BestCrypt.
63. Призначення генератора ключів у системі BestCrypt.
64. Особливості роботи зі Схованим і Оригінальним контейнерами.
65. Системи аутентифікації електронних даних (імітовставка, електронний підпис).
66. Кабінетний замок "Сонет". Система FireWall-1/VPN-1. Система OmniGuard/Enterprise Security Manager компанії Axent.
67. Брандмауери. Мережевий екран PIX Firewall, Cisco PIX, FireWall/Plus – фірми NETWORK-1.
68. Апаратно-програмний комплекс захисту інформації "ШИП", "Dallas Lock".
69. Криптографічний адаптер.
70. Процесор безпеки мережі. Локатори ліній зв'язку. Локатор провідникових ліній "Вектор". Нелінійний радіолокатор NR-900E.
71. Сканер NetRecon.
72. Аналізатор телефонних ліній SP-18/T "Багер-01". Детектор електромагнітного поля Д-006.
73. Зонд-монітори. Зонд-монітор СРМ-700 (Акула).
74. Вимірювачі частот, нелінійні радіолокатори.
75. Ручний вимірювач частот РИЧ-2.

76. Універсальні комплекси моніторингу. Універсальний комплекс моніторингу технічних каналів витоку інформації “КРОНА-6000”.
77. Система NetRecon.
78. Багатофункціональні комплекси захисту. Комплексний пошуковий прилад ST-31 “Пиранья”.
79. Захист приміщень. Система “Полонез”, “Менует”.
80. Портативний пошуковий прилад Д-008.
81. СВЧ-перетворювач (конвертор) ПС-3900, ПС-5700, ПС-6000. Спектральний корелятор OSC-5000 (OSCOR).
82. Засоби управління криптографічними ключами: генерація, зберігання, розподілення ключів.
83. Тестування дисків: компонента Disk Diagnostics Contents, SMARTTests. PartitionTests, a DataAdvisor (Радник Даних), Ontrack JumperViewer, SizeManager, Data Recovery (Відновлення Даних).
84. Основні кроки відновлення даних: компонента AdvancedRecovery, DeletedRecovery, FormatRecovery.
85. Призначення та особливості програми Disk Wiper. Створення нових логічних дисків, їх форматування, перевірка правильності позначення створеного диска. Послідовність очистки вільного простору на диску, повної очистки диску, видалення логічного диска, приховування диска та його відображення.
86. Стратегія захисту інформації у фінансово-економічних інформаційних системах. Комплекс технічних і програмних засобів захисту інформації.
87. Рівні мережевих атак (фізичний, канальний, мережевий, транспортний, сеансовий) згідно моделі OSI.
88. Типи атак (відмова від обслуговування, перебір варіантів, метод соціального інжинірингу, пасивна атака, атака типу “Sniff”, неправильний адрес мережі, “закидання” пакетами, недозволене з’єднання, недозволений протокол, ICMП атака, несанкціоноване адміністрування, зміна пароля, DNS атака, недозволений час і т. п.).
89. Політика ролей.
90. Технології цифрових підписів.
91. Стратегія вибору систем виявлення атак.
92. Термінали захищеної інформаційної системи.
93. Визначення комп’ютера, який працює в мережі у режимі “Sniff”.
94. Загальні відомості про блокові шифри.

95. Мережа Фейштеля.
96. Методи рандомізації повідомлень.
97. Генератори випадкових і псевдовипадкових послідовностей.
98. Алгоритм Хаффмана.
99. Стандарт блокових шифрів AES. Алгоритм RSA.
100. Блоковий шифр TEA. Стандарт DES (Data Encryption Standard).
101. Системи виявлення атак, стратегія вибору.
102. Попередня оцінка конфіденціальності та цінності інформації.
103. Планування витрат часу та засобів на несанкціонований доступ до системи із системним забезпеченням Microsoft Windows і програм пакета Microsoft Office виділення найбільших загроз (несанкціоноване читання, зміна інформації, її вилучення, знищення і т. п.).
104. Побудова моделі захисту системи, визначення витрат часу ресурсів і засобів.
105. Засіб протоколювання процесів Syslog.
106. Стійкість паролів проти злому, програма Crack.
107. Файл паролів /etc/passwd. Програма демон (daemon), яка виконує прослуховування повідомлень відповідної служби.
108. Захист режимів Telnet, FTP, Network File System, протоколу POP, агента передачі повідомлень Sendmail, сервера HTTP.
109. Система пошуку та захисту від вторгнення LIDS (Linux Intrusion Detection/Defence System).
110. Заборона та обмеження доступу до файлів, пам'яті, систем комп'ютера, мережевих інтерфейсів, програм, що працюють, встроєного детектора сканування портів тощо.
111. Призначення та формати файлів LIDS.cap, LIDS.net, LIDS.pw, LIDS.conf, $PGDATA/passwd, /etc/services. Вибір паролів і прав доступу до системи.
112. Багаторівнева аутентифікація. Утиліти Crack5.0 та John The Ripper.
113. Механізм доступу до інформації — програмні закладки. Програма Crack.
114. Механізм захисту в Linux типу "маскарадінг". Перекомпіляція ядра для включення захисту типу "маскарадінг".
115. Система OpenSSH, яка шифрує весь трафік (включаючи паролі).

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

СПИСОК ЛІТЕРАТУРИ

Основна

1. *Домарев В. В.* Безопасность информационных технологий. — СПб.: DiaSoft, 2002. — 688 с.
2. *Защита* компьютерных систем от разрушающих программных воздействий: Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 128 с.
3. *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.
4. *Конев И., Беляев А.* Информационная безопасность предприятия. — СПб.: БХВ Петербург, 2003. — 752 с.
5. *Методы* и средства защиты информации / Под ред. Ю. С. Ковтанюка. — К.: ЮНИОР, 2003. — 501 с.

Додаткова

6. *О вирусах*, червях, троянцах и бомбах. Защита информании: Переводы. — М.: Знание, 1990. — Новое в жизни, науке и технике. Сер. “Вычислительная техника и ее применение”.
7. *Касперский Е.* “Дыры” в MS-DOS и программы защиты информации. — М.: Компьютер-Пресс, 1991.
8. *Баранов А. П., Зегжда Д. П., Зегжда П. Д. и др.* Теоретические основы информационной безопасности: Учеб. пособие. — СПб., 1998. — 173 с.
9. *Жельников В.* Криптография от папируса до компьютера. — М.: ABF, 1996.
10. *Галатенко В. А., Гагин А. В.* Информационная безопасность — обзор основных положений, Jet INFO, # 1,2,3. — М., 1996. — Ч. 1–3.
11. *Герасименко В. А., Размахнин М. К.* Криптографические методы в автоматизированных системах // Зарубежная радиоэлектроника. — 1982. — № 8.

12. *Головкин Б. А.* Надежное программное обеспечение (обзор) // Зарубежная радиоэлектроника. — 1978. — № 12. — С. 3–61.
13. *Давыдовский А. И.* Использование средств автоматизации, заслуживающих доверие // Защита информации. — 1992. — № 1. — С. 63–71.
14. *Месси Дж. Л.* Введение в современную криптологию // ТИИЭР. — 1988. — Т. 76. — № 5. — С. 24–42.
15. *Джефф П. Р.* Шифрование данных методом гаммирования // Электроника. — 1973. — Т. 46. — № 1.
16. *Защита* программного обеспечения / Пер. с англ. Д. Гроувер, Р. Сатер, Дж. Фипс и др.; Под ред. Д. Гроувера. — М.: Мир, 1992. — 285 с.
17. *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.
18. *Зегжда П. Д., Копылов Д. Ю., Корт С. С. и др.* Защита информации в компьютерных системах: Лабораторный практикум // Под ред. проф. П. Д. Зегжды. — СПб., 1996. — 89 с.
19. *Касперский Е.* Компьютерные вирусы в MS-DOS. — М.: Эдэль, 1992. — 120 с.
20. *Клоков Ю. К., Папушин В. К., Хамитов Р. Р.* Методы повышения надежности программного обеспечения // Зарубежная радиоэлектроника. — 1984. — № 6. — С. 3–22.
21. *Коржик В. И., Финк Л. М., Щелкунов К. Н.* Расчет помехоустойчивости систем передачи дискретных сообщений: Справочник. — М.: Радио и связь, 1981. — 232 с.
22. *Краснов А. В.* Некоторые проблемы безопасности в сетях ЭВМ и способы их решения. Защита информации. — 1992. — № 3–4.
23. *Липаев В. В.* Надежность программного обеспечения (обзор концепций) // Автоматика и телемеханика. — 1986. — № 10. — С. 5–31.
24. *Лихарев С. Б.* Базовые средства криптографической защиты информации в ПЭВМ // Защита информации. — 1992. — № 3.
25. *Медведовский И. Д., Безгачев В. А., Юреленков А. П.* Информационная безопасность распределенных вычислительных систем: Руководство к практическим занятиям // Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 73 с.
26. *Перший А. Ю.* Организация защиты вычислительных систем // Компьютер-Пресс. — 1992. — № 10–11. — С. 35–50; 33–42.

27. *Петраков А. В., Лагутин В. С.* Утечка и защита информации в телефонных каналах. — 2-е изд. — М.: Энергоатомиздат, 1997. — 304 с.
28. *Проскуряков А. М.* Интеллектуальная собственность. — Вологда: Ардвисура, 1998.
29. *Расторгуев С. П., Дмитриевский Н. Н.* Искусство защиты и "раздевания" программ. — М.: Совмаркет, 1991. — 60 с.
30. *Ростовцев А. Г., Маховенко Е. Б.* Теоретические вопросы криптологии. Несимметричные криптоалгоритмы и элементы криптоанализа. Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 47 с.
31. *Спесивцев А. В. и др.* Защита информации в персональных компьютерах. — М.: Радио и связь, 1992. — С. 140–149.
32. *Сяо Д., Керр Д., Медник С.* Защита ЭВМ. — М.: Мир, 1982.
33. *Тимофеев Ю. А.* Комплексный подход к защите коммерческой информации (почему и как надо защищать компьютерную систему) // Защита информации. — 1992. — № 1.
34. *Диффи У.* Первые десять лет криптографии с открытым ключом // ТИИЭР. — 1988. — Т. 76. — С. 54–74.
35. *Уайт Д.* Электромагнитная совместимость радиоэлектронных средств и непреднамеренные помехи. — Вып. 3.: Пер. с англ. — М.: Сов. радио, 1979. — 464 с.
36. *Уолкер Б. Дж., Блейк Я. Ф.* Безопасность ЭВМ и организация их защиты. — М.: Связь, 1980.
37. *Хорев А. А.* Способы и средства защиты информации. — М.: МО РФ, 1998. — 316 с.
38. *Хоффман Л. Дж.* Современные методы защиты информации. — М.: Сов. радио, 1980.
39. *Щербаков А.* Построение программных средств защиты от копирования: Практ. рекомендации. — М.: Эдэль, 1992.
40. *Ярочкин В. И.* Безопасность информационных систем. — М.: Ось-89, 1996.
41. *Ярочкин В. И.* Система безопасности фирмы. — М.: Ось-89, 1998.
42. *Ярочкин В. И.* Технические каналы утечки информации. — М.: ИПКИР, 1994. — 105 с.

ЗМІСТ

Відповідальний за випуск *Ю. В. Нешкуренко*
Редактор *Т. М. Тележенко*
Комп’ютерне верстання *М. М. Соколовська*

Зам. № ВКЦ-2669
Міжрегіональна Академія управління персоналом (МАУП)
03039 Київ-39, вул. Фрометівська, 2, МАУП