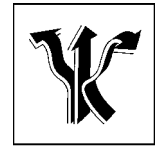
МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ



МЕТОДИЧНІ МАТЕРІАЛИ ЩОДО ЗАБЕЗПЕЧЕННЯ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

з дисципліни

“ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ”

(для бакалаврів)

Київ 2007

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

Затверджено на засіданні кафедри інформатики та інформаційних технологій (протокол № 6 від 02.02.07)

Схвалено Вченою радою Міжрегіональної Академії управління персоналом

Ахрамович В. М. Методичні матеріали щодо забезпечення самостійної роботи студентів з дисципліни "Технології захисту інформації" (для бакалаврів). — К.: МАУП, 2007. — 40 с.

Методичні матеріали містять пояснювальну записку, тематичний план самостійної роботи студентів з дисципліни "Технології захисту інформації", теми рефератів, питання для самоконтролю та співбесіди, тестові завдання (за двома модулями), методичні вказівки до підготовки, написання та захисту реферату, а також список літератури.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Основний зміст самостійної роботи студентів над дисципліною полягає у вивченні та застосуванні системи знань у галузі теорії та практики застосування організаційного, правового, програмно-апаратного, інженерно-технічного забезпечення інформаційної безпеки у сфері професійної та управлінської діяльності, у вивченні та застосуванні документів програмних комплексів, які використовуються при виконанні лабораторних робіт.

До самостійної роботи належать також вивчення та освоєння методичних вказівок до лабораторних робіт і вивчення додаткової літератури, пов'язаної з виконанням цих робіт.

Значну частину самостійної роботи студентів становить вивчення нормативних документів сфери предметної області з організації робіт.

Лише постійне самостійне навчання дає можливість якомога більше наблизитися до вершини знань певної галузі, оволодіти такою сумою знань і вмінь, яка б дала змогу заявити про себе як про професіонала. Студент, який хоче якнайкраще оволодіти професією, має добре розуміти: на занятті викладач подає основи знань, спрямовує студента у процесі навчання, виокремлює ті ключові істини дисципліни, які пробуджують у молодої людини потяг до поглиблення й удосконалення всіх знань. Збагачення загальною сумою знань, накопичених людством, розширення загального світогляду, усвідомлення наявної перспективи щодо реалізації певних знань є основним мотивом сумлінного ставлення до навчання. Самостійна навчальна діяльність студента буде результативною лише тоді, коли вона ґрунтуватиметься на внутрішній потребі. Виховання відповідної здатності у студента потребує чіткого узгодження процесу самоосвіти з цілями навчання та виховання.

Згідно з державними стандартами навчальний матеріал дисципліни, передбачений навчальним планом для засвоєння студентом у процесі самостійної роботи, виноситься на підсумковий контроль поряд з навчальним матеріалом, який опрацьовувався на заняттях. Самостійна робота студента над засвоєнням навчального матеріалу з конкретної дисципліни може виконуватись у бібліотеці вищого навчального закладу, навчальних кабінетах, комп'ютерних класах (лабораторіях), а також у домашніх умовах. Самостійна робота студента повинна бути спланована, організаційно і методично спрямована як особиста

творча праця без безпосередньої взаємодії з викладачем. Навчальний час, відведений для самостійної роботи, регламентується робочим навчальним планом і згідно з Болонською декларацією повинен становити не менше 50 % загального обсягу навчального часу студента, відведеного для вивчення конкретної дисципліни. За потреби ця робота виконується за складеним графіком, що гарантує можливість індивідуального доступу студента до потрібних дидактичних засобів. Графік доводиться до відома студентів на початку поточного семестру. При організації самостійної роботи студентів з використанням складного обладнання чи устаткування, складних систем доступу до інформації (наприклад, комп'ютерних баз даних, систем автоматизованого проектування тощо) передбачається можливість отримання необхідної консультації або допомоги з боку фахівця.

Самостійна навчальна діяльність студента може здійснюватись за такими напрямами:

- запам'ятовування певної інформації за рахунок уважного слухання і конспектування лекцій; активна робота на практичних заняттях;
- робота над конспектами лекцій, планами практичних занять;
- опрацювання літературних джерел (конспектування самостійно вивченого матеріалу, написання реферату);
- робота з каталогами звичайних і електронних бібліотек, інформаційно-пошуковими сервісами мережі Інтернет;
- вивчення навчального матеріалу за паперовими та електронними підручниками, навчальними посібниками, практикумами тощо;
- опрацювання матеріалу за першоджерелами, науковою і спеціальною літературою;
- підготовка доповідей, рефератів, написання курсових робіт; пошукова і науково-дослідна діяльність;
- самотестування.

Самостійна робота студента на лекції. Лекційний матеріал призначається для найраціональнішого спрямування щодо вивчення дисципліни і передбачає акцентування уваги на найскладніших, ключових питаннях дисципліни. Належне ведення конспекту під час лекції сприяє збереженню необхідної інформації та дає студенту змогу в подальшому проаналізувати її. За умови викладу лекційного матеріалу в усній формі одночасно засвоюється до 20 % інформації. Викладання інформатики в комп'ютерних класах або в аудиторіях,

облаштованих мультимедійним обладнанням (наприклад, мультимедійним проектором або сенсорним екраном), з демонстрацією прийомів роботи з користувацьким інтерфейсом програми сприяє підвищенню рівня засвоєння лекційного матеріалу до 60 %.

Робота над конспектами лекцій, планами практичних занять. При підготовці до практичних занять студент має спиратися на складений ним конспект лекції. При опрацюванні матеріалу лекції слід порівняти законспектований матеріал з планом практичного заняття, що міститься у методичних матеріалах для практичних занять або у навчально-методичному комплексі. Якщо в конспекті бракує матеріалу з окремих питань лекції або недостатньо розкриті деякі питання практичного заняття, або вони винесені для самостійного опрацювання, студент повинен звернутися до рекомендованих підручників, навчальних посібників і відповідних методичних матеріалів. Підготовку до практичного заняття краще за все здійснювати з використанням ПЕОМ зі встановленим на ньому відповідним програмним забезпеченням.

Вивчення навчального матеріалу за підручниками, навчальними посібниками, методичними вказівками, опрацювання матеріалу за першоджерелами, науковою і спеціальною літературою. Працювати з підручниками, навчальними посібниками, методичними вказівками, практикумами, науковою і спеціальною літературою незалежно від типу їхнього носія (паперового чи електронного) необхідно так, щоб отримати максимум теоретичних знань і навичок. При роботі з джерелами студент насамперед повинен ознайомитись з їх змістом, щоб визначити, чи необхідно опрацьовувати джерело та чи стосується воно навчального курсу, і тільки після цього визначити послідовність його опрацювання і добрати необхідний для вивчення матеріал з джерела (глави, розділи тощо). У разі роботи з інтерактивними електронними джерелами слід використовувати можливості навігації за документом, що надаються сучасними програмами, призначеними для читання електронних документів відповідних форматів (*MS Word, Adobe Reader, Adobe Acrobat* та ін.) і особливо переваги гіпертекстової технології подання навчального матеріалу, а саме — за допомогою гіперпосилань знаходити відповіді на поставлені запитання. При опрацюванні матеріалу необхідно з'ясувати сутність питання, що вивчається, не уникаючи визначення сутності незрозумілих чи незнайомих слів, термінів. Саме інтерактивні гіпертекстові електронні джерела (довідки у складі програмних продуктів, електрон-

ні посібники та словники) дають змогу конкретизувати терміни та визначення якнайшвидше. При вивченні матеріалу необхідно аналізувати прочитане, порівнюючи з прослуханою та законспектованою лекцією, робити логічні висновки, позначати незрозумілі положення з метою подальшого з'ясування на практичному занятті. Бажано відпрацювати зручну для себе систему позначень (позначки на полях конспекту, підкреслення маркерами різних кольорів, доповнення конспекту альтернативними формулюваннями та посиланнями на інші джерела тощо) та фіксації опрацьованого матеріалу. Сучасні текстові редактори (насамперед *MS Word*) надають можливість створити електронний конспект з примітками, виносками, коментарями та його роздруківкою. Для самостійного поглибленого вивчення навчального матеріалу слід звертатися до наукової та спеціальної літератури, яка може бути і не зазначеною в навчально-методичному комплексі. Використання самостійно отриманих відомостей як у навчанні, так і на практиці є, безперечно, цінним здобутком діяльності студента на шляху формування професійного потенціалу.

Робота з бібліотечними фондами та дистанційними джерелами з метою пошуку необхідної інформації. Знання з технологій захисту інформації належать до базової підготовки сучасної людини. З позицій випереджаючої освіти навчання тільки за конспектом лекцій і основною літературою, зазначеною у навчальній програмі, є недостатнім. У більшості випадків належна підготовка вимагає вмінь швидко знаходити та опрацьовувати необхідний матеріал за першоджерелами, науковою і спеціальною літературою та коректно цитувати знайдене. Перелік такої літератури, як правило, наводиться у навчально-методичному комплексі навчальної дисципліни. Тому завдання студента зводиться до самостійного знаходження цих матеріалів шляхом пошуку у паперових або електронних фондах бібліотек, а також у файлових архівах, базах даних і базах знань, доступ до яких здійснюється за допомогою відповідних сервісів Інтернету (зокрема *Word Wide Web, FTP* та *UseNet newsgroups*).

Для пошуку документа використовуються різні його ознаки. У першу чергу це — реквізити (УДК, автор(и), заголовок опису, основний заголовок: відомості, що стосуються заголовка / відомості про відповідальність, відомості про видання (у тому числі URL-адреса web-документа або Ftp-файла), місце та дата видання, обсяг.) УДК — це універсальна десяткова класифікація офіційних видань у всьому світі. Відповідні довідники видаються багатьма мовами і пос-

тійно оновлюються. В Україні у 2006 р. Книжкова палата України ім. Івана Федорова видала "Універсальну десяткову класифікацію. Зміни та доповнення" (вип. 4) у паперовому варіанті. Довідкова база УДК постійно нарощується за рахунок електронних видань. Знання УДК дає змогу швидко знайти необхідне джерело за систематичним бібліотечним каталогом. Наприклад, УДК видань з інформаційних технологій починається з 004.

Якщо код УДК невідомий, необхідно звернутися до алфавітного каталогу бібліотеки і за назвою джерела або прізвищем та ініціалами автора знайти відповідний бібліотечний шифр джерела.

Якщо ж студент здійснює наукове дослідження вибраної проблеми, готує наукову доповідь або виступ на конференції і йому не відомі реквізити джерела або саме джерело, то слід зробити пошук у систематичному бібліотечному каталозі. Завдання студента полягає у пошуку необхідної галузі (підгалузі), що охоплює розшукувану інформацію, а потім у межах цієї галузі (підгалузі) — картки з необхідним джерелом і бібліотечним шифром. У подальшому студент повинен оформити бібліотечне замовлення на літературу встановленого зразка, до якого внести шифр знайденого джерела та необхідні реквізити. Робота з електронними фондами в цьому варіанті значно ефективніша, оскільки у сучасних бібліотеках облік літератури ведеться в середовищах систем управління базами даних, за допомогою яких пошук потрібної інформації здійснюється найефективніше.

Сервіси мережі Інтернет надають унікальні можливості знаходження літературних джерел у географічно віддалених фондах та архівах, а також шляхом участі у мережних конференціях, де можна отримати відповіді та поради щодо питань з розшукуваної інформації. Для доступу до Інтернет-ресурсів необхідно знати їх мережну адресу. Оскільки Інтернет постійно оновлюється і розвивається, в ньому немає єдиного каталога, змісту або наочного покажчика ресурсів. Проте в Інтернеті існують різні інформаційно-пошукові системи, що допомагають користувачам знайти те, що їм потрібно. Це насамперед тематичні каталоги і так звані пошукові машини. Тематичні (наочні) каталоги — це інформаційно-довідкові системи, підготовлені вручну редакторами цих систем на основі інформації, зібраної на серверах Інтернету. Інформація в цих системах розподіляється за тематичними розділами відповідно до певної ієрархії. На верхньому рівні розділів зібрано загальні категорії (наприклад, "Інтернет", "Бізнес", "Мистецтво", "Освіта" тощо), на нижньому — посилання на конкретні

web-сторінки або інші інформаційні ресурси. Для швидкого переходу до потрібного розділу тематичного каталогу можна скористатися вбудованою системою автоматичного пошуку за ключовими словами. Для цього в рядку запиту слід ввести ключове слово (поєднання слів), клацнути ***Пошук***, і система повідомить, чи є відповідний розділ у її каталозі та запропонує перейти в нього, обминувши проміжні розділи. Рекомендуємо використовувати каталоги: http://www.yahoo.com, http://www.portal.edu.ru, http://www.ipl.org.

Пошукові системи є складними інформаційно-довідковими системами, що автоматично генеруються на основі даних, які збираються мережними програмами-роботами по всій мережі Інтернет, і надають у відповідь на запит користувача посилання на різні Інтернет-ресурси. Запит здійснюється за певною процедурою (певною мовою), яка може відрізнятися в різних системах, проте у спрощеному вигляді вона зводиться до того, що користувач вводить у спеціальному полі (або в кількох полях) ключові слова та/або словосполучення, що найточніше відображають суть проблеми.

До загальних положень мов запитів належать:

- Ключові слова можна вводити у відповідне поле пошукової системи поодинці, послідовно звужуючи пошук, або одразу кілька слів, розділяючи їх пробілами або комами. Регістр не має значення.
- Режим пошуку "AND" ("І") означає, що буде знайдено тільки ті дані, де зустрічається кожне з ключових слів.
- При використанні режиму "OR" ("АБО") результатом пошуку будуть усі дані, де зустрічається хоч би одне ключове слово.
- Використовуйте знаки "+" і "–" перед ключовим словом. Щоб виключити документи, де зустрічається певне слово, поставте перед ним знак "–". І навпаки, щоб певне слово обов'язково було в документі — поставте перед ним знак "+". Зверніть увагу, що між знаком і словом не повинно бути пропуску.
- Якщо ви хочете виключити яке-небудь слово з пошуку, поставте перед ним знак "–". Наприклад: "+захист –Excell".
- За замовчуванням програма шукає всі дані, де зустрічається введене вами слово. Наприклад, при запиті "редактор" будуть знайдені слова "редактор", "текстовий", "графічний", "газети", "головний" і багато інших. Знак оклику перед або після ключового слова означає, що будуть знайдені тільки слова точно відповідні запиту (наприклад, "текстовий! редактор!").

Також корисно запам'ятати і використовувати при пошуку такі прийоми:

- Якщо для пошуку потрібно ввести словосполучення, укладіть його в лапки.
- Якщо ви пишете все слово рядковими літерами, будуть знайдені всі варіанти його написання; якщо ви позначили хоч би одну літеру в шуканому слові великою, то система шукатиме тільки такі варіанти.
- Якщо ви хочете знайти не текст, а яке-небудь зображення, то можна користуватися словом image. Наприклад, image:sea дасть список сторінок із зображенням моря.
- Якщо слово, яке ви шукаєте, зустрічається в різних контекстах, можна виключити слова, які зустрічаються в непотрібному контексті. Наприклад, вказати аргумент пошуку +Celeron +Price +UA –USA.
- Перевіряйте орфографію. Якщо пошук не дав результатів, можливо, при введенні ви припустилися помилки.
- Використовуйте синоніми. Якщо список знайдених сторінок дуже малий або не містить корисних сторінок, спробуйте змінити слово. Наприклад, замість "реферати", можливо, більше підійде "курсові роботи" або "твори".
- Якщо один із знайдених документів ближчий до шуканої теми, ніж інші, клацніть Знайти схожі документи. Це посилання розташоване під короткими описами знайдених документів. Система проаналізує сторінку і знайде документи, схожі на ті, які ви зазначили.

Подібних систем в Інтернеті значно більше, ніж тематичних каталогів. Серед пошукових систем існують як широкі за тематикою метапошукові системи, так і вузькоспеціалізовані. Найвідоміші з них: http://www.google.com, http://www.altavista.com, http://www.askjeeves.com, http://www.lycos.com, http://www.sciseek.com, http://www.msn.com, http://meta.ua, http://www.rambler.ru, http://www.yandex.ru, http://www.aport.ru, http://www.metabot.ru, http://newsgroups.langenberg.com, uk.wikipedia.org, www.bukinist.agava.ru.

Матеріали щодо методів підвищення ефективності пошуку інформації в Інтернеті містяться у статтях: http://www.yandex.ru/info/search.html, http://www.searchengines.ru/, http://www.zodchiy.ru/links/search/, http://www.citforum.ru/internet/search/index.shtml,

http://websearch.report.ru/, http://www.kokoc.com/search-engines/index.shtml, http://www.zhurnal.ru/search-r.shtml.

Самостійна робота має такі складові і форми їх оцінювання:

- підготовка та власне аудиторна робота під час практичних і лабораторних занять. Результати її оцінюються під час поточного контролю;
- виконання самостійних робіт у формі есе, рефератів з конкретних проблем і складання письмових звітів на електронних або паперових носіях, або усних доповідей;
- опрацювання програмного матеріалу зі змістового модуля та оцінювання його результатів під час проміжного контролю;
- виконання письмової контрольної роботи або тестування;
- звіт про проходження практики;
- звіт про науково-дослідну роботу, результати якої можуть бути використані при написанні випускної роботи і за рішенням кафедри опубліковані.

У результаті самостійного вивчення навчальної дисципліни "Технології захисту інформації" 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; керівні документи, що визначають ступінь захищеності комп'ютерних систем; методи проведення аналізу надійності системи захисту інформації в комп'ютерних системах; основні методи, технологію, принципи і правила побудови захисту електронних обчислювальних машин, у тому числі персональних комп'ютерів, їх елементів і об'єктів комп'ютерних мереж;
- мати досить повне уявлення про алгоритми створення сучасних програм, алгоритми кодування та застосування стандартного програмного забезпечення захисту; методи та 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 конфіденційних документів; роботи із системами й методами визначення захищеності носіїв інформації; створення засобами

стандартного програмного забезпечення елементів захисту інформації; формулювати задачі з питань захисту інформації та, формалізуючи їх, зазначати шляхи вирішення.

ТЕМИ САМОСТІЙНОЇ РОБОТИ ЗА МОДУЛЕМ І

№ теми	Назва розділу, теми курсу	Зміст завдання	Форми контролю
1	2	3	4
Модуль І. Менеджмент інформаційної безпеки			
1	Категорії інформаційної безпеки з погляду інформації та інформаційних систем	1. Етапи розвитку систем захисту. 2. Основні загрози інформаційній безпеці. 3. Категорії безпеки інформації та інформаційних систем. 4. “Помаранчева книга” США	Конспект
2	Абстрактні моделі захисту інформації. Огляд найбільш поширених методів “злому”	1. Абстрактні моделі захисту інформації. 2. Побудова моделі захисту системи, визначення затрат часу, ресурсів і засобів. 3. Огляд найбільш поширених методів “злому”. 4. Комплексний пошук можливих методів доступу. 5. Термінали захищеної інформаційної системи	Конспект
3	Класи безпеки. Критерії інформаційної безпеки. Канали витоку інформації	1. Класи безпеки інформації та інформаційних систем. 2. Класифікація систем за критеріями інформаційної безпеки	Конспект

1	2	3	4
		3. Вимоги щодо роботи з конфіденційною інформацією. 4. Створення політики інформаційної безпеки 5. Електромагнітні та електричні канали витоку інформації. 6. Параметричні канали витоку інформації	
4	Класифікація криптоалгоритмів	1. Тайнопис, криптографія з ключем. 2. Симетричні та асиметричні криптоалгоритми	Конспект
5	Системи шифрування даних, які передаються в мережах	1. Канальне шифрування. 2. Абонементне шифрування	Конспект
6	Засоби управління криптографічними ключами	1. Генерація ключів. 2. Зберігання і розподілення ключів	Конспект
Реферат			

ТЕМИ РЕФЕРАТІВ ЗА МОДУЛЕМ І

1. Категорії інформаційної безпеки.

Література [1; 3; 4]

2. Абстрактні моделі захисту інформації.

Література [4; 5; 8; 10; 17]

3. Огляд найбільш поширених методів “злому” інформаційних систем.

Література [1–7; 17–19; 26; 29; 31]

4. Класи безпеки. Критерії інформаційної безпеки.

Література [1–5; 10; 23; 33; 41]

5. Канали витоку інформації.

Література [13; 27; 35; 40; 42]

6. Криптоалгоритми.

Література [2; 5; 11; 14; 15; 24; 30; 34]

7. Системи шифрування даних в мережах.
Література [2; 5; 11; 14; 15; 24; 30; 34]
8. Управління ключами.
Література [11; 14; 15; 24; 30; 34]
9. Електромагнітні та електричні канали витоку інформації.
Література [13; 27; 35; 40; 42]
10. Параметричні канали витоку інформації.
Література [13; 27; 35; 40; 42]

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ТА СПІВБЕСІДИ ЗА МОДУЛЕМ І

1. Категорії інформаційної безпеки з погляду інформації та інформаційних систем.
2. Технічні, програмно-апаратні та адміністративні засоби захисту інформації.
3. Визначення об'єкта захисту та можливих загроз.
4. Принцип розімкнутого управління, компенсації, зворотного зв'язку.
5. Відповідальність за протиправні дії згідно із законодавством України.
6. Ідентифікація й аутентифікація. Механізми підзвітності та аудиту.
7. Класи безпеки.
8. Критерії інформаційної безпеки.
9. Канали витоку інформації.
10. Класифікація інформації за рівнем конфіденційності.
11. Класифікація криптоалгоритмів.
12. Тайнопис, криптографія з ключем, симетричні та асиметричні криптоалгоритми. Скремблери.
13. Мережа Фейштеля.
14. Перестановочні, підстановочні криптоалгоритми.
15. Поточні, блочні шифри. Одиниці кодування.
16. Системи шифрування дискових даних (системи прозорого та спеціального видів шифрування).
17. Системи шифрування даних, які передаються в мережах (канальне та абонементне шифрування).

ТЕСТОВІ ЗАВДАННЯ ЗА МОДУЛЕМ І

1.1. Можливості обходу пароля в BIOS:

a. застосувати “пароль чорного ходу” виробника BIOS;
b. використовувати програму злому пароля;
c. скинути CMOS за допомогою перемички або перемикання контактів;
d. скинути CMOS видаленням акумулятора не менш ніж на 10 хв;
e. заміна BIOS на аналогічну модель.

1.2. Можливості користувача із правами адміністратора:

a. не може встановлювати програми й устаткування, але має доступ до вже встановлених на комп’ютері програм;
b. може змінювати власний малюнок, призначений обліковому запису, а також створювати, змінювати або видаляти власний пароль;
c. не може змінювати ім’я або тип власного облікового запису. Такі зміни повинні виконуватися користувачем з обліковим записом адміністратора комп’ютера;
d. може створювати й видаляти облікові записи користувачів на комп’ютері;
e. може створювати паролі для інших користувачів на комп’ютері;
f. може змінювати в обліковому записі імена користувачів, малюнки, паролі й типи облікових записів;
g. не може змінити тип свого облікового запису в разі, коли на комп’ютері більше немає користувачів з обліковим записом адміністратора комп’ютера.

1.3. Можливості користувача з обмеженими правами:

a. не може встановлювати програми й устаткування, але має доступ до вже встановлених на комп’ютері програм;
b. може змінювати власний малюнок, призначений обліковому запису, а також створювати, змінювати або видаляти власний пароль;
c. не може змінювати ім’я або тип власного облікового запису. Такі зміни повинні виконуватися користувачем з обліковим записом адміністратора комп’ютера;
d. може створювати й видаляти облікові записи користувачів на комп’ютері;

e. може створювати паролі для інших користувачів на комп'ютері;
f. може змінювати в обліковому записі імена користувачів, малюнки, паролі й типи облікових записів;
g. не може змінити тип свого облікового запису в разі, коли на комп'ютері більше немає користувачів з обліковим записом адміністратора комп'ютера.

1.4. У паролі для Windows символи: ~ ! @ # $ % ^ & * ( ) _ + — = { } | [ ] \ : "; ' < > ?, . / використовувати:

a. можна;
b. не можна.

1.5. Кількість символів у паролі Windows XP не повинна перевищувати такої кількості знаків:

a. 256;
b. 127;
c. 14.

1.6. У режимі захисту від збоїв операційна система Windows використовує настроювання за замовчуванням:

a. монітор VGA;
b. підтримка мережі відсутня;
c. драйвер миші Microsoft і мінімальний набір драйверів пристроїв;
d. читання компакт-дисків, принтерів.

1.7. Функції Брандмауера Windows XP:

a. допомагає підвищити безпеку комп'ютера;
b. створює дискету скидання паролів;
c. обмежує інформацію, що надходить у комп'ютер з інших комп'ютерів;
d. дає змогу краще контролювати дані на комп'ютері й забезпечує лінію оборони комп'ютера від людей або програм (включаючи віруси й хропаки).

1.8. Для проглядання списку активних портів комп'ютера вводиться команда з командного рядка:

a. Netstat –c;
b. Netstat –o;
c. Netstat –a.

1.9. У програмі Microsoft Excel встановити захист на окремі комірки, не використавши команди для захисту листа (аркуша):

a. можна;
b. не можна.

1.10. Етапів захисту інформації є:

a. три;
b. шість;
c. десять;
d. два.

1.11. Етапи захисту інформації початковий і розвинений характеризуються:

a. комплексним шляхом розвитку;
b. екстенсивним шляхом розвитку.

1.12. Стосовно засобів захисту в Росії визначено:

a. десять класів захищеності;
b. сім класів захищеності;
c. шість класів захищеності.

1.13. Стосовно засобів захисту в США визначено:

a. десять класів захищеності;
b. сім класів захищеності;
c. шість класів захищеності.

1.14. Небезпечні дії на комп'ютерну інформаційну систему можна поділити на:

a. навмисні;
b. не навмисні;
c. випадкові;
d. злочинні.

1.15 Причинами випадкових дій при експлуатації можуть бути:

a. незадоволеність службовця своєю кар'єрою;
b. хабар;
c. цікавість;
d. конкурентна боротьба;

e. прагнення самотверджуватися за будь-яку ціну;
f. аварійні ситуації, спричинені стихійними лихами і відключеннями електроживлення;
g. відмови й збої апаратури;
h. помилки в програмному забезпеченні;
i. помилки в роботі персоналу;
j. перешкоди в лініях зв'язку через дії зовнішнього середовища.

1.16. Дії порушника можуть бути обумовлені такими мотивами:

a. незадоволеністю службовця своєю кар'єрою;
b. хабарем;
c. цікавістю;
d. конкурентною боротьбою;
e. прагненням самоствердуватися за будь-яку ціну;
f. аварійними ситуаціями, спричиненими стихійними лихами і відключеннями електроживлення;
g. відмовами й збоями апаратури;
h. помилками в програмному забезпеченні;
i. помилками в роботі персоналу.

1.17. Гіпотетична модель потенційного порушника інформаційної безпеки:

a. кваліфікація порушника на рівні розробника певної системи;
b. порушник вибирає найбільш сильну ланку в захисті;
c. порушником може бути стороння особа;
d. порушником може бути законний користувач системи;
e. порушником може бути власник інформації;
f. порушнику відома інформація про принципи роботи системи;
g. порушник вибирає найбільш слабку ланку в захисті.

1.18. Навмисні дії, спрямовані на порушення інформаційної безпеки, можна поділити на:

a. перехоплення;
b. розкрадання;
c. модифікацію;
d. руйнування.

1.19. Класифікація каналів несанкціонованого доступу, за якими можна здійснити розкрадання, зміну або знищення інформації, можлива:

a. через людину;
b. через програму;
c. через апаратуру.

1.20. Заходи з формування режиму інформаційної безпеки можна поділити на такі рівні:

a. законодавчий (закони, нормативні акти, стандарти тощо);
b. морально-етичний (норми поведінки, недотримання яких призводить до падіння престижу конкретної людини або цілої організації);
c. адміністративний (дії загального характеру, організації, що чиняться керівництвом);
d. фізичний (механічні, електро- і електронно-механічні перешкоди на можливих шляхах проникнення потенційних порушників);
e. апаратно-програмний (електронні пристрої й спеціальні програми захисту інформації).

1.21. При організації захисту бази даних розроблювач повинен визначити паролі для таких облікових записів:

a. обліковий запис користувача “Admin” (для активізації діалогового вікна Вхід);
b. обліковий запис користувача, що є власником бази даних і таблиць, які містяться в ній, запитів, форм, звітів і макросів;
c. будь-який обліковий запис користувача, доданий у групу “Admins”.

1.22. Символи “ \ [ ] : | < > + = ; , . ? * для паролів баз даних використовувати:

a. можна;
b. не можна.

1.23. Програмою Microsoft Access захист сторінок доступу до баз даних:

a. забезпечується;
b. не забезпечується.

1.24. Програма BestCrypt використовує алгоритм шифрування:

a. алгоритм Blowfish;
b. Twofish алгоритм;
c. ГОСТ 28147-89.

1.25. Алгоритм Blowfish був розроблений:

a. Брюсом Шнеїром разом із Джоном Келсеєм, Крис Хол, Нілсом Фергузоном, Девідом Уогнером і Дугом Вікінгом;
b. Джоаном Даєменом і Вінсентом Риджменом;
c. Брюсом Шнеїром.

1.26. Алгоритм Twofish був розроблений:

a. Брюсом Шнеїром разом із Джоном Келсеєм, Крис Хол, Нілсом Фергузоном, Девідом Уогнером і Дугом Вікінгом;
b. Джоаном Даєменом і Вінсентом Риджменом;
c. Брюсом Шнеїром.

1.27. Контейнер для шифрування може використовувати програма:

a. Super File Encryption;
b. T-CEC Pro;
c. BestCrypt.

1.28. Програма Windows Disk Wiper використовується для:

a. шифрування інформації;
b. видалення інформації;
c. створення логічного диску.

1.29. Основні причини пошкоджень електронної інформації розподілилися згідно з даними дослідницького центру DataPro Research таким чином:

a. ненавмисна помилка людини — 52 % випадків;
b. ненавмисна помилка людини — 12 % випадків;
c. умисні дії людини — 10 % випадків;
d. умисні дії людини — 60 % випадків;
e. відмова техніки — 10 % випадків;
f. відмова техніки — 30 % випадків;
g. пошкодження в результаті пожежі — 15 % випадків;
h. пошкодження в результаті пожежі — 45 % випадків;

i. пошкодження водою — 10 % випадків;
j. пошкодження водою — 60 % випадків.

1.30. Дії зловмисників, які дістались до інформації:

a. у 44 % випадків злому були проведені безпосередні крадіжки грошей з електронних рахунків;
b. у 14 % випадків злому були проведені безпосередні крадіжки грошей з електронних рахунків;
c. у 16 % випадків виводилося з ладу програмне забезпечення;
d. у 46 % випадків виводилося з ладу програмне забезпечення;
e. у 12 % випадків інформація була сфальсифікована;
f. у 92 % випадків інформація була сфальсифікована;
g. у 10 % випадків зловмисники за допомогою комп'ютера скористалися або замовили послуги, до яких у принципі не повинні були мати доступу;
h. у 80 % випадків зловмисники за допомогою комп'ютера скористалися або замовили послуги, до яких у принципі не повинні були мати доступу.

1.31. Конфіденційність інформації — гарантія того, що:

a. конкретна інформація доступна тільки тому колу осіб, для якого вона призначена. Порушення цієї категорії називається розкраданням або розкриттям інформації;
b. інформація зараз існує у її початковому вигляді, тобто при її зберіганні або переданні не було несанкціонованих змін. Порушення цієї категорії називається фальсифікацією повідомлення;
c. джерелом інформації є саме та особа, яка заявлена як її автор. Порушення цієї категорії також називається фальсифікацією, але вже автора повідомлення.

1.32. Цілісність інформації — гарантія того, що:

a. конкретна інформація доступна тільки тому колу осіб, для якого вона призначена. Порушення цієї категорії називається розкраданням або розкриттям інформації;
b. інформація зараз існує у її початковому вигляді, тобто при її зберіганні або переданні не було проведено несанкціонованих змін. Порушення цієї категорії називається фальсифікацією повідомлення;
c. джерелом інформації є саме та особа, яка заявлена як її автор.

Порушення цієї категорії також називається фальсифікацією, але вже автора повідомлення.

1.33. Автентичність інформації — гарантія того, що:

a. конкретна інформація доступна тільки тому колу осіб, для якого вона призначена. Порушення цієї категорії називається розкраданням або розкриттям інформації;
b. інформація зараз існує в її початковому вигляді, тобто при її зберіганні або переданні не було проведено несанкціонованих змін. Порушення цієї категорії називається фальсифікацією повідомлення;
c. джерелом інформації є саме та особа, яка заявлена як її автор. Порушення цієї категорії також називається фальсифікацією, але вже автора повідомлення.

1.34. Стосовно інформаційних систем застосовуються категорії:

a. надійність;
b. точність;
c. контроль доступу;
d. контрольованість;
e. контроль ідентифікації;
f. стійкість до умисних збоїв.

1.35. Надійність інформаційних систем — це гарантія того, що:

a. система поводиться в нормальному й позаштатному режимах так, як заплановано;
b. буде здійснено точне й повне виконання всіх команд;
c. різні групи осіб мають різний доступ до інформаційних об'єктів, і ці обмеження доступу постійно виконуються;
d. у будь-який момент може бути здійснена повноцінна перевірка будь-якого компонента програмного комплексу;
e. клієнт, підключений у певний момент до системи, є саме тим, за кого себе видає;
f. при умисному внесенні помилок у межах наперед обумовлених норм система поводитиметься так, як обумовлено наперед.

1.36. Контроль доступу інформаційних систем – це гарантія того, що:

a. система поводиться в нормальному й позаштатному режимах так, як заплановано;
b. різні групи осіб мають різний доступ до інформаційних об'єктів, і ці обмеження доступу постійно виконуються;
c. у будь-який момент може бути проведена повноцінна перевірка будь-якого компонента програмного комплексу;
d. клієнт, підключений у певний момент до системи, є саме тим, за кого себе видає;
e. при умисному внесенні помилок у межах наперед обумовлених норм система поводитиметься так, як обумовлено наперед.

1.37. На теорії автоматів заснована модель абстрактного захисту інформації:

a. модель Біба (Biba);
b. модель захисту Сазерлендська (від англ. Sutherland);
c. модель Гогена-Мезігера (Goguen-Meseguer);
d. модель захисту Кларка-Вільсона (Clark-Wilson).

1.38. На використанні трансакцій і ретельному оформленні прав доступу суб'єктів до об'єктів заснована модель абстрактного захисту інформації:

a. модель Біба (Biba);
b. модель захисту Сазерлендська (від англ. Sutherland);
c. модель Гогена-Мезігера (Goguen-Meseguer);
d. модель захисту Кларка-Вільсона (Clark-Wilson).

1.39. На дослідженні поведінки множинних композицій функцій переходу з одного стану в інший заснована модель абстрактного захисту інформації:

a. модель Біба (Biba);
b. модель захисту Сазерлендська (від англ. Sutherland);
c. модель Гогена-Мезігера (Goguen-Meseguer);
d. модель захисту Кларка-Вільсона (Clark-Wilson).

1.40. Ідея дешифрування шифру типу "Скитала" належить:

a. Сократу;
b. Чемберлену;
c. Аристотелю;
d. Цузе.

1.41. Криптографія — це:

a. пошук і дослідження математичних методів перетворення інформації;
b. дослідження можливості розшифрування інформації без знання ключів.

1.42. Криптоаналіз — це:

a. пошук і дослідження математичних методів перетворення інформації;
b. дослідження можливості розшифрування інформації без знання ключів.

1.43. При оцінці ефективності шифру зазвичай керуються правилом:

a. Аристотеля;
b. Керкхоффа;
c. Курчатова;
d. Лейбніца.

1.44. Приклади алфавітів шифрування, які використовуються в сучасних ІС:

a. алфавіт Z33 — 32 літери російського алфавіту й пропуск;
b. алфавіт Z256 — символи, що входять до стандартних кодів ASCII і КОИ-8;
c. бінарний алфавіт — Z2 = {0,1};
d. вісімковий алфавіт або шістнадцятковий.

1.45. Авторами алгоритму RSA є:

a. Райвест, Шамір і Адлеман — Rivest, Shamir, Adleman (розкладання великих чисел на прості множники);
b. Діффі й Хелман. Обчислення логарифма або зведення в ступінь.

1.46. Авторами алгоритму DH є:

a. Райвест, Шамір і Адлеман — Rivest, Shamir, Adleman (розкладання великих чисел на прості множники);
b. Діффі й Хелман. Обчислення логарифма або зведення в ступінь.

1.47. Алгоритм DES використовує ключ:

a. завдовжки 56 біт;
b. завдовжки 256 біт.

1.48. Алгоритм ГОСТ 28147-89 використовує ключ:

a. завдовжки 56 біт;
b. завдовжки 256 біт.

1.49. Скремблерами називаються:

a. перетворення блоку вхідної інформації фіксованої довжини й одержання результуючого блоку того ж об'єму, але недоступного для прочитання стороннім персонам, які не володіють ключем;
b. програмні або апаратні реалізації алгоритму, що дає змогу шифрувати побітно безперервні потоки інформації.

1.50. Основою, на якій реалізовані практично всі сучасні криптосистеми, є шифри:

a. блокові;
b. потокові.

1.51. Як параметр V для будь-якого із блокових перетворень може використовуватися:

a. фіксоване число (наприклад, X′=X+125);
b. число, що отримується з ключа (наприклад, X′=X+F(Key));
c. число, що отримується з незалежної частини блоку (наприклад, X2′=X2+F(X1)).

1.52. У схемі, названою ім'я її творця — мережею Фейштеля, використовується такий варіант блокових перетворень:

a. фіксоване число (наприклад, X′=X+125);
b. число, що отримується з ключа (наприклад, X′=X+F(Key);
c. число, що отримується з незалежної частини блоку (наприклад, X2′=X2+F(X1)).

1.53. Блоковими є алгоритми:

a. IDEA;
b. CAST128;
c. BlowFish;
d. TwoFish;
e. MARS.

1.54. Безліч сучасних методів захисних перетворень можна поділити на такі групи:

a. заміни (підстановки);
b. перестановки;
c. адитивні (гамування);
d. комбіновані методи.

ТЕМИ САМОСТІЙНОЇ РОБОТИ ЗА МОДУЛЕМ II

№ теми	Назва розділу, теми курсу	Зміст завдання	Форми контролю
1	2	3	4
Модуль II. Менеджмент безпеки інформаційних систем			
7	Сучасна ситуація у сфері інформаційної безпеки. Рівні мережних атак	1. Рівні мережних атак згідно з моделлю OSI. 2. Захист систем передавання інформації	Конспект
8	Апаратні та програмні засоби захисту інформації в мережах	1. Системи ідентифікації й аутентифікації користувача (традиційні та біометричні параметри). 2. Система FireWall-1/VPN-1 . Система OmniGuard/Enterprise Security Manager компанії Axent. 3. Брандмауери, Мережний екран PIX Firewall. 4. Апаратно-програмний комплекс захисту інформації “ШИП”, “Dallas Lock”. 5. Криптографічний адаптер. Процесор безпеки мережі. Локатори ліній зв’язку. 6. Сканер NetRecon. 7. Аналізатор телефоних ліній SP-18/T “Багер-01”. 8. Детектор електромагнітного поля Д-006	Конспект

1	2	3	4
9	Термінали захищеної інформаційної системи. Отримання пароля на основі помилок	1. Термінали захищеної інформаційної системи. 2. Отримання пароля на основі помилок адміністратора та користувача.	Конспект
		3. Отримання пароля на основі помилок у реалізації. 4. Соціальна психологія та інші способи отримання пароля	
Реферат			

ТЕМИ РЕФЕРАТІВ ЗА МОДУЛЕМ ІІ

1. Сучасна ситуація у сфері інформаційної безпеки.
   Література [1–8; 12; 13; 19; 22–24; 26; 42]
2. Рівні мережних атак.
   Література [5; 17; 37; 39]
3. Захист систем передавання інформації.
   Література [1–8; 16; 18–23; 26; 27; 31; 35–42]
4. Апаратні та програмні засоби захисту інформації в мережах.
   Література [1–8; 16; 18–23; 26; 27; 31; 35–42]
5. Системи ідентифікації й аутентифікації користувача.
   Література [1; 3; 5]
6. Брандмауери та мережні екрани.
   Література [1; 3; 5]
7. Термінали захищеної інформаційної системи.
   Література [1–8; 16; 18–23; 26; 27; 31; 35–42]
8. Отримання пароля на основі помилок систем захисту.
9. Аутентифікація та ідентифікація.
   Література [1; 3; 5]
10. Відновлення даних.
    Література [1–6; 11; 20; 23; 29; 32; 37]

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ТА СПІВБЕСІДИ ЗА МОДУЛЕМ ІІ

1. Системи аутентифікації електронних даних (імітовставка, електронний підпис).
2. Засоби управління криптографічними ключами: генерація, зберігання і розподілення ключів.
3. Стратегія захисту інформації у фінансово-економічних інформаційних системах.
4. Комплекс технічних і програмних засобів захисту інформації.
5. Сучасна ситуація у сфері інформаційної безпеки.
6. Рівні мережних атак (фізичний, канальний, мережний, транспортний, сеансовий) згідно з моделлю OSI.
7. Типи атак.
8. Вимоги до роботи з конфіденційною інформацією.
9. Політика ролей. Технології цифрових підписів.
10. Стратегія вибору систем виявлення атак.
11. Термінали захищеної інформаційної системи.
12. Отримання пароля на основі помилок адміністратора та користувача.
13. Отримання пароля на основі помилок у реалізації. Соціальна психологія та інші способи отримання пароля.
14. Побудова моделі захисту системи, визначення затрат часу ресурсів і засобів.
15. Система пошуку та захисту від вторгнення LIDS.
16. Створення дерева каталогів із правами доступу. Зміна змісту каталогу access.conf .
17. Добавлення користувача та встановлення його прав.
18. Служби, які можуть захищати від кібероблав.
19. Установлення та зміна паролів, контроль доступу в систему, права користувачів.

ТЕСТОВІ ЗАВДАННЯ ЗА МОДУЛЕМ ІІ

2.1. Термінали захищеної інформаційної системи — це:

a. комп'ютери;
b. точки входу користувача в інформаційну мережу;
c. клавіатура;
d. порти.

2.2. При використанні терміналів із фізичним доступом необхідно дотримуватися таких вимог:

a. захищеність терміналу має відповідати захищеності приміщення: термінали без пароля можуть бути лише в тих приміщеннях, куди мають доступ особи відповідного або вищого рівня доступу. Відсутність імені реєстрації можлива тільки в тому разі, якщо до терміналу має доступ лише одна людина, або якщо на групу осіб, які мають до нього доступ, поширюються загальні заходи відповідальності. Термінали, установлені в публічних місцях, повинні завжди робити запит на ім'я реєстрації й пароль;
b. системи контролю за доступом у приміщення зі встановленим терміналом повинні працювати повноцінно й відповідно до загальної схеми доступу до інформації;
c. у разі установки терміналу в місцях із широким скупченням народу клавіатура, а якщо необхідно, то й дисплей повинні бути обладнані пристроями, що дають змогу бачити їх тільки працюючому в певний момент клієнту (непрозорі скляні або пластмасові огорожі, шторки, "втоплена" модель клавіатури).

2.3. Паролі можуть зберігатися у відкритому текстовому вигляді в операційній системі:

a. UNIX;
b. Windows;
c. Novell NetWare.

2.4. Паролі можуть зберігатися у вигляді малозначних контрольних сум (хеш-значень) в операційній системі:

a. UNIX;
b. Windows;
c. Novell NetWare.

2.5. До класу 0 належить інформація:

a. недоступна у відкритому вигляді, але її розкриття не призведе до небезпеки;
b. загальнодоступна інформація;
c. розкриття якої призведе до значних втрат на ринку;
d. розкриття якої призведе до фінансової загибелі компанії.

2.6. До класу 1 належить інформація:

a. недоступна у відкритому вигляді, але її розкриття не призведе до небезпеки;
b. загальнодоступна інформація;
c. розкриття якої призведе до значних втрат на ринку;
d. розкриття якої призведе до фінансової загибелі компанії.

2.7. До класу 2 належить інформація:

a. недоступна у відкритому вигляді, але її розкриття не призведе до небезпеки;
b. загальнодоступна інформація;
c. розкриття якої призведе до значних втрат на ринку;
d. розкриття якої призведе до фінансової загибелі компанії.

2.8. До класу 3 належить інформація:

a. недоступна у відкритому вигляді, але її розкриття не призведе до небезпеки;
b. загальнодоступна інформація;
c. розкриття якої призведе до значних втрат на ринку;
d. розкриття якої призведе до фінансової загибелі компанії.

2.9. На етапі аналізу таблиці ризиків перевіряються такі дані:

a. визначається середньоквадратичне відхилення ризику;
b. перевіряється кожен рядок таблиці на неперевищення ризику визначеного значення;
c. здійснюється порівняння подвоєного значення з інтегральним ризиком;
d. визначається середньоарифметичне значення ризику.

2.10. Атака на сервери здійснюється на таких рівнях OSI (Open Systems Interconnection):

a. транспортному;
b. фізичному;
c. канальному;
d. мережному;
e. сеансовому.

2.11. Апаратно-програмні засоби захисту інформації можна поділити на такі групи:

a. системи ідентифікації (розпізнавання) і аутентифікації (перевірки достовірності) користувачів;
b. системи шифрування дискових даних;
c. системи шифрування даних, передаваних за мережами;
d. системи аутентифікації електронних даних;
e. засоби управління криптографічними ключами.

2.12. Для реалізації імітовставки використовується принцип:

a. симетричного шифрування;
b. асиметричного шифрування;

2.13. Для реалізації електронного підпису використовується принцип:

a. симетричного шифрування;
b. асиметричного шифрування.

2.14. Традиційними системами вважаються такі, що засновані на таких типах даних:

a. секретній інформації, якою володіє користувач (пароль, секретний ключ, персональний ідентифікатор тощо). Користувач повинен запам'ятати цю інформацію або ж для неї можуть бути застосовані спеціальні засоби зберігання;
b. фізіологічних параметрах людини (відбитки пальців, малюнок райдужної оболонки ока тощо) або особливості поведінки (особливості роботи на клавіатурі тощо).

2.15. Біометричними системами вважаються такі, що засновані на таких типах даних:

a. секретній інформації, якою володіє користувач (пароль, секретний ключ, персональний ідентифікатор тощо). Користувач повинен запам'ятати цю інформацію або ж для неї можуть бути застосовані спеціальні засоби зберігання;
b. фізіологічних параметрах людини (відбитки пальців, малюнок райдужної оболонки ока тощо) або особливості поведінки (особливості роботи на клавіатурі тощо).

2.16. Формула K=max(int(N*0.1*3)+1, 3) визначає:

a. кількість дозволених спроб клієнта на вхід у систему, після чого його вхід у систему блокується;
b. кількість дозволених спроб клієнтів на вхід у систему, після чого система блокується.

2.17. У момент відправлення пакета підтвердження або відкидання пароля в системі повинна бути встановлена розумна затримка:

a. 2–5 секунд;
b. 2–5 хвилин;
c. 2–5 годин.

2.18. Паролі можуть зберігатися у вигляді малозначних контрольних сум (хеш-значень) в операційній системі:

a. UNIX;
b. Windows;
c. Novell NetWare.

2.19. Основні методи боротьби з копіюванням паролів:

a. адекватний захист робочих станцій від запуску сторонніх програм спеціальних драйверів, які блокують запуск здійснимих файлів без відома оператора або адміністратора;
b. відключення змінних носіїв інформації (гнучких дисків);
c. монітори, що повідомляють про будь-які зміни системних налагоджень і списку програм, що автоматично запускаються;
d. система одноразових паролів (при кожній реєстрації в системі клієнтам із дуже високим рівнем відповідальності самою системою генерується новий пароль).

2.20. Незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, що призвело до перекручення чи знищення комп'ютерної інформації, або носіїв такої інформації, а також поширення комп'ютерного вірусу через застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини, системи чи комп'ютерні мережі й здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації, караються:

a. штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на термін до двох років, або

обмеженням волі на такий самий термін;
b. штрафом від п'ятдесяти до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на термін до двох років;
c. штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян, позбавленням права обіймати певні посади чи займатися певною діяльністю на термін до п'яти років, або виправними роботами на термін до двох років.

2.21. Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства, чи зловживання службовим становищем караються:

a. штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян, виправними роботами на термін до двох років, або обмеженням волі на такий самий термін;
b. штрафом від п'ятдесяти до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на термін до двох років;
c. штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян, позбавленням права обіймати певні посади, чи займатися певною діяльністю на термін до п'яти років, або виправними роботами на термін до двох років.

2.22. Порушення правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж особою, яка відповідає за їх експлуатацію, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту, або незаконне копіювання комп'ютерної інформації, або істотне порушення роботи таких машин, їх систем чи комп'ютерних мереж, караються:

a. штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян, виправними роботами на термін до двох років або обмеженням волі на такий самий термін;
b. штрафом від п'ятдесяти до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на термін до двох років;
c. штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян, позбавленням права обіймати певні посади чи займатися певною діяльністю на термін до п'яти років, або виправними роботами на термін до двох років.

2.23. Незаконні дії з документами на переказ платіжними картками та іншими засобами доступу до банківських рахунків обладнанням для їх виготовлення караються:

a. штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян, виправними роботами на термін до двох років або обмеженням волі на такий самий термін;
b. штрафом від п'ятдесяти до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на термін до двох років;
c. штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян, позбавленням права обіймати певні посади, чи займатися певною діяльністю на термін до п'яти років, або виправними роботами на термін до двох років;
d. штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на термін до трьох років.

МЕТОДИЧНІ ВКАЗІВКИ ДО ПІДГОТОВКИ, НАПИСАННЯ ТА ЗАХИСТУ РЕФЕРАТУ

Реферат є складовою вивчення дисципліни.

Ці завдання підготовлено відповідно до курсу "Технології захисту інформації" для бакалаврів.

Мета написання реферату — допомогти студентам засвоїти теоретичні знання, розвинути й удосконалити навички захисту інформації, використання сучасних нових інформаційних технологій у сфері захисту (пакетів прикладних програм) і засобів обчислювальної техніки.

Оформлення й захист рефератів повинні сприяти активному засвоєнню нового матеріалу, виробленню у студентів уміння комплексного використання суміжних дисциплін при вирішенні практичних питань.

Структура реферату

План (розділи)	Обсягу	Короткий зміст (що потрібно висвітлити)
Вступ	Одна сторінка	Мета, загальна характеристика, визначення номера варіанта завдання
Назва кожного питання відповідно до реферату	Одна-дві старінки	Викладення суті питання з наведенням прикладів і посилань на літературні джерела
Висновки	Одна сторінка	Прикладне значення
Список використаної літератури	Одна сторінка	
Додатки	Одна-три стрінки	

Загальний обсяг реферату — 30 сторінок друкованого тексту через 2 інтервали, рукописного — до 24 сторінок шкільного зошита.

Виконання та оформлення реферату

Студент повинен виконати реферат, розкривши історичні передумови певної проблеми, відповідаючи на всі питання теоретичного плану, і описати технологію розв'язання практичної задачі, якщо така передбачена рефератом.

Відповіді на теоретичні питання потребують ретельної роботи з літературою. Крім виписок і конспектування з літературних джерел, наприклад, з Інтернету, студент повинен зробити висновки. Робота має бути виконана самостійно. У тексті реферату потрібно робити посилання на використану літературу. У висновках загалом з реферату розглядають питання економічної доцільності і практичного застосування сучасних інформаційних технологій та обчислювальної техніки у сфері захисту.

Реферат потрібно оформляти на стандартних аркушах паперу, зброшурованих у папку. Усі аркуші мають бути пронумеровані. На титульній сторінці необхідно зазначити назву вищого навчального

закладу, факультет, спеціальність, дисципліну, курс, групу, а також прізвище, ініціали та номер залікової книжки.

На першій сторінці потрібно навести розрахунок варіанта контрольної роботи та питання варіанта і проставити номери сторінок, на яких викладено цей матеріал. На останній сторінці студент підписує роботу і ставить дату. У кінці роботи необхідно зазначити використану літературу. Зшита папка має бути вкладена в поліетиленовий файл і містити дискету з повним текстом, графікою тощо набраного варіанта реферату.

Вибір варіанта реферату

Кожний студент отримує окреме завдання для виконання КР згідно з варіантом Z, який обчислюється за формулою

$$Z = \mathrm{mod}_{10}(NZK + PR - 2000) + 1,$$

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

Наприклад, NZK = 398, PR = 2001, тоді

$$Z = \mathrm{mod}_{10}(398 + 2001 - 2000) + 1 = \mathrm{mod}_{10}(399) + 1 = 9 + 1 = 10.$$

Отже, Z = 10.

Зауваження. 1. Обчислення варіанта має бути наведене у вступі до контрольної роботи.

2. Для довідки: $\mathrm{mod}_a b$ дорівнює залишку від ділення b на a.

Увага!

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

Індивідуально-консультаційна робота

Індивідуально-консультаційна робота з дисципліни здійснюється у формі консультацій за графіком (одна консультація на два тижні). На консультаціях студентам надаються пояснення з виконання самостійної роботи, підготовки до практичних занять, перевірки та захисту реферату.

Мета вивчення дисципліни:

1. Оволодіння студентами комплексом знань у сфері захисту інформації, системами й методами визначення захищеності програмних продуктів, пристроїв; комп'ютерних мереж, їх складових і набуття на основі цих знань практичних навичок і теоретичних знань, необхідних для творчого підходу в питанні

сучасного та майбутнього оперативного захисту комп'ютерної техніки й інформації.

2. Оволодіння студентами алгоритмами створення сучасних програм захисту; алгоритмами кодування; сучасними методами, технологією; комп'ютерними програмними, технічними засобами у сфері захисту: операційних систем, текстових редакторів, табличних процесорів, систем управління базами даних, конфіденційної інформації тощо. Набуття на основі одержаних знань практичних навичок, необхідних для розробки систем захисту, керування розробкою систем захисту, наслідком чого є нормальне забезпечення роботи фінансових організацій, регіонів країни зі збереженням характеристик трафіку, швидкості санкціонованого доступу тощо.
3. Оволодіння концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденційних документів; стратегією вибору систем виявлення атак, навичками роботи з пристроями безпеки в локальних і глобальних комп'ютерних мережах із метою використання їх можливостей для покращання показників безпеки.

СПИСОК ЛІТЕРАТУРИ

Основна

1. *Домарев В. В.* Безопасность информационных технологий. — СПб.: DiaSoft, 2002. — 688 с.
2. *Защита* компьютерных систем от разрушающих программных воздействий / Под ред. проф. П. Д. Зегжды: Руководство к практ. занятиям. — СПб., 1998. — 128 с.
3. *Зегжда Д. П., Калинин М. О., Степанов П. Г.* Теоретические основы информационной безопасности. Защищенные операционные системы: Руководство к практ. 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 информации. Переводы. — М.: Знание, 1990. (Новое в жизни, науке и технике. Сер. "Вычислительная техника и ее применение", с. 9).

7. *Касперский Е.* “Дыры” в MS-DOS и программы защиты информации // КомпьютерПресс. — 1991. — № 10.
8. *Баранов А. П., Зегжда Д. П., Зегжда П. Д. и др.* Теоретические основы информационной безопасности (Дополнительные главы): 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 (ч. 1–3) // Jet INFO. — 1996. — № 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. — М.: Мир, 1988.
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 практ. 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: Лаборатор. 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., Гореленков А. П.* Информационная безопасность распределенных вычислительных систем: Руководство к практ. занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 73 с.
26. *Перший А. Ю.* Организация защиты вычислительных систем // КомпьютерПресс. — 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 практ. 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. — М.: Мир, 1988. — С. 54–74.
35. *Уайт Д.* Электромагнитная совместимость радиоэлектронных средств и непреднамеренные помехи: Пер. с англ. — М.: Сов. радио, 1979. — Вып. 3. — 464 с.
36. *Уолкер Б. Дж., Блейк Я. Ф.* Безопасность ЭВМ и организация их защиты. — М.: Радио и 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

Пояснювальна записка 3
Теми самостійної роботи за модулем I 11
Теми рефератів за модулем I 12
Питання для самоконтролю та співбесіди за модулем I 13
Тестові завдання за модулем I 14
Теми самостійної роботи за модулем II 25
Теми рефератів за модулем II 26
Питання для самоконтролю та співбесіди за модулем II 27
Тестові завдання за модулем II 27
Методичні вказівки до підготовки, написання
та захисту реферату 33
Список літератури 36

Відповідальний за випуск *А. Д. Вегеренко*
Редактор *О. В. Лебідь*
Комп'ютерне верстання *О. А. Залужна*

Зам. № ВКЦ-3036
Міжрегіональна Академія управління персоналом (МАУП)
03039 Київ-39, вул. Фрометівська, 2, МАУП