МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

МЕТОДИЧНІ МАТЕРІАЛИ ЩОДО ЗАБЕЗПЕЧЕННЯ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

з дисципліни

“ІНФОРМАЦІЙНА БЕЗПЕКА”

(для магістрів)

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 дисциплін "Інформаційна безпека" (для магістрів). — К.: МАУП, 2007. — 42 с.

Методичні матерали містять пояснювальну записку, теми самостійної роботи, методичні вказівки до підготовки, написання та захисту реферату, а також список літератури.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Те, що інформація має цінність, люди усвідомили дуже давно — недаремно листування сильних світу цього одвіку було об'єктом пильної уваги їх ворогів і друзів. Тоді й постало завдання захисту листування від надмірно цікавих. Стародавні люди намагалися використовувати для вирішення цього завдання найрізноманітніші методи, і одним з них був тайнопис — уміння складати повідомлення так, щоб його зміст був недоступний нікому, окрім посвячених у таємницю. Відомі свідоцтва, що мистецтво тайнопису зародилося ще за доантичних часів. Упродовж усієї багатовікової історії аж до недавніх часів це мистецтво служило небагатьом, здебільшого верхівці суспільства, не виходячи за межі резиденцій держав, посольств і, звичайно ж, розвідувальних місій. І лише кілька десятиліть тому все докорінно змінилося — інформація дістала самостійну комерційну цінність і стала доволі поширеним, майже звичайним товаром. Її зберігають, транспортують, продають і купують, а отже, крадуть і підроблюють, а тому вона потребує захисту. Сучасне суспільство дедалі більшою мірою стає інформаційно зумовленим. Успіх будь-якого виду діяльності щодалі значніше залежить від володіння певними відомостями і від відсутності їх у конкурентів. І що сильніше виявляється цей ефект, то значніші потенційні збитки від зловживань в інформаційній сфері і, отже, потреба в захисті інформації.

У сучасному суспільстві для задоволення його потреб постають проблеми інформаційного забезпечення всіх сфер діяльності людини. Однією з цих проблем є забезпечення надійного захисту інформації. Особливої гостроти вона набуває у зв'язку з масовою комп'ютеризацією всіх видів діяльності людини, об'єднанням ЕОМ у комп'ютерні мережі та підключення до мережі Інтернет. Вибір серед великої кількості сучасних методів і засобів захисту таких, що найбільшою мірою відповідають конкретним умовам діяльності та забезпечують достатній рівень безпеки становить доволі складне завдання, особливо для початківців. Разом з тим для багатьох технологій захисту існує велика кількість спільних рис як щодо розробки, так і використання. Це дає можливість вивчати сучасні технології на прикладах, які, незважаючи на новизну, вже стали класичними. До таких технологій належать засоби захисту операційної системи, мережні екрани, криптографічні системи, системи визначення атак та реакцій на них, системи моніторингу інформаційної безпеки. При цьому вивчення цих технологій спирається на ґрунтовну теоретичну базу і

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.

Основний зміст самостійної роботи студентів полягає у вивченні та використанні системи знань у галузі теорії та практики застосування організаційного, правового, програмно-апаратного, інженерно-технічного забезпечення інформаційної безпеки у сфері професіональної та управлінської діяльності, у вивченні документів програмних комплексів, які застосовуються при виконанні лабораторних робіт, а також у вивченні та освоєнні методичних вказівок до виконання лабораторних робіт і аналізі відповідної додаткової літератури.

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

Лише постійне самостійне навчання дає можливість досягти вершин знань з певної галузі, опанувати такий обсяг знань і вмінь, який би дав змогу заявити про себе як професіонала. Студент, який бажає якомога краще оволодіти професією, повинен усвідомити: на занятті викладач подає базові засади знань, навчає, як учити, виокремлює ключові поняття дисципліни з метою пробудження потягу до поглиблення й удосконалення знань. Збагачення загальною сумою знань, накопичених людством, розширення загального світогляду, усвідомлення перспективи щодо реалізації певних знань є основним мотивом для сумлінного ставлення до навчання. Самостійна навчальна діяльність студента лише тоді буде результативною, коли базуватиметься на внутрішній потребі. Виховання відповідної здатності потребує чіткого узгодження процесу самоосвіти з цілями навчання.

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;
- роботу 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;
- підготовку доповідей, рефератів, написання курсових робіт; пошукова і науково-дослідна діяльність;
- самотестування.

Самостійна робота студента на лекції. Лекційний матеріал призначається для найраціональнішого спрямування студентів 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 студентам 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 свій конспект лекції. При опрацюванні матеріалу лекції слід порівняти законспектований матеріал з планом практичного заняття, що міститься в методичних матеріалах для практичних занять або в навчально-методичному комплексі. Якщо в конспекті бракує матеріалу з окремих питань лекції або недостатньо розкрито деякі питання практичного заняття, або вони мають бути опрацьовані самостійно, студент повинен звернутися до рекомендованих підручників, навчальних посібників і відповідних методичних матеріалів. Підготовку до практичного заняття найкраще 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 якнайбільший обсяг теоретичних знань і навичок. При роботі з джерелами студент насамперед повинен ознайомитися з їх змістом, щоб визначити, чи необхідно опрацьовувати джерело та чи стосується воно навчального курсу, і тільки після цього визначити послідовність його опрацювання і відібрати необхідний для вивчення матеріал з джерела (глави, розділи тощо). При роботі з інтерактивними електронними джерелами слід використовувати можливості навігації за документами, 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, електронні посібники та словники) сприяють конкретизації термінів і визначень. 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 роздрукувати його. Для самостійного поглибленого вивчення навчального матеріалу слід звертатися до наукової та спеціальної літератури, на яку може й не вказуватися в навчально-методичному комплексі. Використання самостійно отриманих відомостей як у навчанні, так і на практиці, безперечно, є 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, вказаною в навчальній програмі, недостатнє. У більшості випадків належна підготовка передбачає вміння швидко знаходити та опрацьовувати необхідний матеріал за першоджерелами, науковою і спеціальною літературою та коректне цитування знайденого. Перелік такої літератури, як правило, наводиться в навчально-методичному комплексі дисципліни. Тому завдання студента зводиться до самостійного знаходження цих матеріалів шляхом пошуку в 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, насамперед — реквізити (УДК, автор(и), заголовок опису, основний заголовок: відомості, що належать до 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 в усьому світі. Відповідні довідники видаються багатьма мовами і постійно оновлюються. 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 невідомі реквізити джерела або власне джерело, слід здійснювати 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 за встановленим зразком, до якого внести шифр знайденого джерела та необхідні реквізити. Робота з електронними фондами в цьому варіанті значно ефективніша, оскільки в сучасних бібліотеках облік літератури здійснюється в середовищах систем управління базами даних, за допомогою яких найлегше знайти потрібну інформацію.

Сервіси мережі Інтернет надають унікальні можливості знаходити літературні джерела у географічно віддалених фондах та архівах, а також шляхом участі в 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, він не містить єдиного каталогу, змісту або наочного покажчика ресурсів. Проте в ньому містяться різні інформаційно-пошукові системи, за допомогою яких користувач може знайти те, що 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 в її каталозі та запропонує перейти в нього, обминувши всі 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 в мережі Інтернет і дають у відповідь на запит користувача посилання на різні Інтернет-ресурси. Запит здійснюється за певними процедурами (певною мовою), що можуть різнитися в різних системах, проте спрощено виглядає так: користувач вводить у спеціальному полі (або в кількох полях) ключові слова та/або словосполучення, що найточніше відбивають сутність проблеми.

До загальних положень мов запитів належать такі.

- Ключові слова можна вводити у відповідне поле пошукової системи поодинці, послідовно звужуючи пошук, або ж 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.
- Слід використовувати знаки "+" і "–" перед ключовим словом. Щоб виключити документи, де зустрічається певне слово, необхідно поставити перед ним знак "–". І навпаки, щоб певне слово обов'язково було в документі, — поставити перед ним знак "+". Зверніть увагу, що між знаком і словом не повинно бути пропуску.
- Якщо необхідно виключити якесь слово з пошуку, поставте перед ним знак "–". Наприклад: "+захист –Excell".
- За замовчуванням програма шукає всі дані, де зустрічається введене слово. Наприклад, при запиті "редактор" будуть знайдені слова "редактор", "текстовий", "графічний", "газети", "головний" та багато інших. Знак оклику перед або після ключового слова означає, що будуть знайдені тільки слова, що точно відповідають запиту (наприклад, "текстовий! редактор!").

Доцільно запам'ятати і використовувати при пошуку такі прийоми.

- Якщо для пошуку потрібно ввести словосполучення, візміть його в лапки.
- Якщо написати все слово малими літерами, будуть знайдені всі варіанти його написання; якщо хоча б одну літеру в шуканому слові написати великою, то система шукатиме тільки такі варіанти.

- Якщо слід знайти не текст, а зображення, то можна користуватися словом image. Наприклад, image: sea дасть список сторінок із зображенням моря.
- Якщо шукане слово 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 було зроблено помилку.
- Використовуйте синоніми. Якщо список знайдених сторінок дуже малий або не містить корисних сторінок, спробуйте змінити слово. Наприклад, замість "реферати", можливо, підійде "курсові роботи" або "твори".
- Якщо один із знайдених документів ближчий до шуканої теми, ніж інші, слід клацнути ***Знайти схожі документи***. Це посилання розташовано під короткими описаннями знайдених документів. Система проаналізує сторінку і знайде документи, схожі на вказані.

Подібних систем в мережі Інтернет значно більше, ніж тематичних каталогів. Серед пошукових систем існують як широкі з тематики метапошукові системи, так і вузькоспеціалізовані. Найвідоміший з них такі: 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 та форми оцінювання:

- підготовка та власне аудиторна робота під час практичних і лабораторних занять. Її результати оцінюються під час поточного контролю;
- виконання самостійних робіт у формі есе, рефератів з конкретних проблем і складання письмових звітів на електронних або паперових носіях чи усних доповідей;
- опрацювання програмного матеріалу зі змістового модуля та оцінка 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 написані випускної роботи і за рішенням кафедри опубліковані.

Мета вивчення дисципліни:

- опанувати комплекс знань у галузі захисту інформації, системи та методи визначення захищеності програмних продуктів, пристроїв; комп'ютерних мереж, їх складових і сформувати на основі здобутих знань практичні навички, необхідні для творчого підходу до питань сучасного оперативного захисту комп'ютерної техніки й інформації;
- вивчити алгоритми створення сучасних програм захисту; алгоритми кодування; сучасні методи, технології; комп'ютерні програмні, технічні засоби в галузі захисту: операційні системи, текстові редактори, табличні процесори, системи управління базами даних, конфіденційної інформації тощо; сформувати навички з розробки систем захисту, управління розробкою систем захисту, забезпечення роботи фінансових організацій, регіонів країни зі збереженням характеристик трафіку, швидкості санкціонованого доступу тощо;
- оволодіти концептуальними моделями розробки, розподілу, опрацювання, використання та зберігання конфіденційних 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.

У результаті самостійного вивчення дисципліни "Інформаційна безпека" студенти повинні:

- знати джерела і способи дії загроз на об'єкти інформаційної безпеки установ, правові та нормативні акти, які визначають систему захисту інформації в державі; керівні документи, що визначають ступінь захищеності комп'ютерних систем; методи 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 достатньо 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;

- сформувати навички роботи з концептуальними моделями розробки, розподілу, опрацювання, використання та зберігання конфіденційних документів; із системами й методами визначення захищеності носіїв інформації; створення засобами стандартного програмного забезпечення елементів захисту інформації; формулювати завдання з питань захисту інформації та, формалізуючи їх, вказувати шляхи розв'язання.

ТЕМИ САМОСТІЙНОЇ РОБОТИ

Номер теми	Назва розділу, теми курсу	Зміст завдання	Форма контролю
1	2	3	4
Модуль І. Менеджмент захисту інформації			
1	Основні положення інформаційної безпеки	1. Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. 2. Категорії інформаційної безпеки. 3. Незаконні дії з документами на переказ, платіжними картками та іншими засобами дос-тупу до банківських рахунків, інших фінансових установ, обладнанням для їх виготовлення	Конспект
2	Апаратно-програмні засоби захисту інформації	1. Визначення каналів витоків інформації, їх типи, особливості. 2. Системи ідентифікації й аутентифікації користувача (традиційні та біометричні параметри). 3. Системи аутентифікації електронних даних (імітовставка, електронний підпис).	Конспект

Продовження таблиці

		4. Брандмауери, мережний екран PIX Firewall. 5. Апаратно-програмний комплекс захисту інформації “ШИП”, “Dallas Lock”. 6. Процесор безпеки мережі. 7. Локатори ліній зв’язку. Локатор провідникових ліній “Вектор”. Нелінійний радіолокатор NR-900E. Сканер NetRecon. Аналізатор телефонних ліній SP-18/T “Багер-01”. 8. Детектор електромагнітного поля Д-006 9. Зонд-монітори. Зонд-монітор СРМ-700 (“Акула”). 10. Універсальний комплекс моніторингу технічних каналів витоку інформації “КРОНА-6000”. 11. Система NetRecon. Багатофункціональні комплекси захисту	Конспект
3	Визначення політики безпеки. Абстрактні моделі захисту інформації	1. Абстрактні та формальні моделі захисту інформації. 2. Особливості моделей Белла-Ла Падуя та Біба	Конспект
4	Захист мереж на основі операційних систем Linux та UNIX	1. Засіб протоколювання процесів Syslog. 2. Стійкість паролів проти зламування, програма Crack. Файл паролів /etc/passwd. 3. Програма демон (daemon) для прослуховування повідомлень відповідної служби. Захист режимів Telnet, FTP, Network File System, протоколу POP, агента передавання повідомлень Sendmail, сервера HTTP.	Конспект

Закінчення таблиці

		4. Система пошуку та захисту від вторгнення LIDS (Linux Intrusion Detection/Defence System)	
5	Законодавча база в галузі захисту інформації	1. Закони України “Про інформацію”, “Про захист інформації в автоматизованих системах”. 2. Вимоги вітчизняних стандартів захисту конфіденційної інформації від несанкціонованого доступу при опрацюванні в автоматизованих системах. 3. Зарубіжна нормативна база в галузі технічного захисту інформації. “Оранжева книга” безпеки. Критерії, вимоги та категорії систем безпеки цієї книги	Конспект
Реферат			

ТЕМИ РЕФЕРАТІВ

1. Канали витоку інформації.
   Література [13; 27; 35; 40; 42]
2. Електромагнітні та електричні канали витоку інформації.
   Література [13; 27; 35; 40; 42]
3. Брандмауери та мережні екрани.
   Література [1; 3; 5]
4. Термінали захищеної інформаційної системи.
   Література [1–8; 16; 18–23; 26; 27; 31; 35–42]
5. Отримання паролю на основі помилок систем захисту.
   Література []
6. Параметричні канали витоку інформації.
   Література [13; 27; 35; 40; 42]
7. Категорії інформаційної безпеки.
   Література [1; 3; 4]
8. Абстрактні моделі захисту інформації.
   Література [4; 5; 8; 10; 17]
9. Найпоширеніші методи “зламування” інформаційних систем.
   Література [1–7; 17–19; 26; 29; 31]

10. Класи безпеки. Критерії інформаційної безпеки.
Література [1–5; 10; 23; 33; 41]
11. Сучасна ситуація в галузі інформаційної безпеки.
Література [1–8; 12; 13; 19; 22–24; 26; 42]
12. Рівні мережних атак.
Література [5; 17; 37; 39]
13. Захист систем передавання інформації.
Література [1–8; 16; 18–23; 26; 27; 31; 35–42]
14. Апаратні та програмні засоби захисту інформації в мережах.
Література [1–8; 16; 18–23; 26; 27; 31; 35–42]
15. Зарубіжна нормативна база в галузі технічного захисту інформації.
Література [1–6; 36; 40]
16. Відновлення даних.
Література [1–6; 11; 20; 23; 29; 32; 37].

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ТА ДИСКУСІЇ

1. Термінали захищеної інформаційної системи.
2. Отримання пароля на основі помилок адміністратора та користувача.
3. Отримання пароля на основі помилок реалізації. Соціальна психологія й інші способи отримання пароля.
4. Побудова моделі захисту системи; визначення затрат часу ресурсів і засобів.
5. Система пошуку та захисту від вторгнення LIDS.
6. Служби, які можуть захищати від кібероблав.
7. Встановлення та зміна паролів, контроль доступу в систему, права користувачів.
8. Завдання моніторингу систем інформаційної безпеки.
9. Модель оптимізації режиму моніторингу систем інформаційної безпеки.
10. Критерії оптимізації режиму моніторингу систем інформаційної безпеки.
11. Як розрахувати необхідний рівень захисту програмного продукту від несанкціонованого використання?
12. Канали витоку інформації.
13. Що таке мережний екран? Його основні функції.
14. Типові компоненти мережних екранів.
15. Обмеження функціонування мережі, пов'язані з використанням брандмауерів.

16. Класифікація мережних екранів.
17. Типова політика використання мережних екранів.
18. Коротка характеристика популярних брандмауерів.
19. Рівні мережних атак (фізичний, канальний, мережний, транспортний, сеансовий) згідно з моделлю OSI.
20. Типи атак.
21. Спільне та відмінне у зовнішніх атаках на комп'ютерну систему від атак "зсередини".
22. Що таке програма типу "троянський кінь"?
23. Галузь використання програм фальшивої реєстрації. Як вони реалізуються?
24. Як здійснюється аутентифікація користувачів за допомогою одноразових паролів?
25. Як здійснюється аутентифікація користувачів за допомогою фізичних об'єктів?
26. Як здійснюється аутентифікація користувачів за допомогою біометричних даних?
27. Загрози інформації.
28. Що таке загроза цілісності даних?
29. Що таке загроза доступності інформації?
30. Що таке загроза несанкціонованого доступу до даних?
31. Сучасні моделі захищених інформаційних систем.
32. Зміст моделі захисту Белла-Ла Падуля.
33. Зміст моделі захисту Біба.
34. Зміст політики безпеки захищеної системи.
35. Відповідальність за протиправні дії згідно із законодавством України.
36. Основні положення Закону України "Про захист інформації в автоматизованих системах" щодо організації захисту інформації.
37. Загальні вимоги до захисту інформації відповідно до Закону України "Про захист інформації в автоматизованих системах".
38. Категорії інформаційної безпеки щодо інформації та інформаційних систем.
39. Технічні, програмно-апаратні та адміністративні засоби захисту інформації.
40. Визначення об'єкта захисту та можливих загроз.
41. Ідентифікація й аутентифікація. Механізми підзвітності та аудиту.
42. Класи безпеки.
43. Критерії інформаційної безпеки.

44. Стратегія захисту інформації у фінансово-економічних інформаційних системах.
45. Комплекс технічних і програмних засобів захисту інформації.
46. Сучасна ситуація в галузі інформаційної безпеки.
47. Класифікація інформації за рівнями конфіденційності.
48. Вимоги при роботі з конфіденційною інформацією.
49. Створення дерева каталогів із правами доступу. Зміна змісту каталогу access.conf.
50. Додавання користувача та встановлення його прав.
51. Як можна використати помилку "переповнення буфера" для атаки на комп'ютерну систему?
52. Основні компоненти комплексної системи захисту інформації.
53. Зміст критеріїв оцінки рівня; безпеки інформації.
54. Типові механізми захисту інформації.
55. Як можна запобігти спробі несанкціонованого копіювання прикладної програми з компакт-диску?
56. Як можна запобігти спробі несанкціонованого копіювання прикладної програми з дискети?
57. Як можна запобігти спробі несанкціонованого копіювання текстової інформації?
58. Як здійснюється захист програм від вивчення?
59. Як здійснюється аналіз програмних реалізацій?

Тести

1.1. Для перегляду списку активних портів комп'ютера вводиться така команда з командного рядка:

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

1.2. Зазначте можливості обійти пароль в BIOS:

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

1.3. Зазначте, чи можна використовувати в паролі для Windows символи ~ ! @ # $ % ^ & * () _ + - = { } | []. \: «; ‘ < > ?,. /:

a) так;
b) ні.

1.4. Кількість символів у паролі Windows XP не повинна перевищувати:

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

1.5. 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.

1.6. Функції брандмауера Windows XP такі:

a) допомагає підвищити безпеку комп’ютера;
b) створює дискету скидання паролів;
c) обмежує інформацію, що надходить на комп’ютер з інших комп’ютерів;
d) сприяє кращому контролю даних на комп’ютері й забезпечує лінію оборони комп’ютера від нападників або програм (включаючи віруси й “хробаків”).

1.7. Зазначте можливості користувача з 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 власного облікового запису, якщо на комп'ютері більше немає користувачів з обліковим записом адміністратора комп'ютера.

1.8. Зазначте 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 власного облікового запису, якщо на комп'ютері більше немає користувачів з обліковим записом адміністратора комп'ютера.

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

a) так;
b) ні.

1.10. Зазначте кількість етапів захисту інформації:

a) три;
b) шість;
c) десять;
d) два.

1.11. Початковий і розвинений етапи захисту інформації характеризуються:

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

1.12. Стосовно засобів захисту в Росії визначено таку кількість класів захищеності:

a) десять;
b) сім;
c) шість.

1.13. Стосовно засобів захисту у США визначено таку кількість класів захищеності:

a) десять;
b) сім;
c) шість.

1.14. Розрізняють такі небезпечні дії на комп'ютерну інформаційну систему:

a) навмисні;
b) ненавмисні;
c) випадкові;
d) злочинні.

1.15. Причинами випадкових дій при експлуатації є такі:

a) незадоволеність службовця кар'єрою;
b) хабар;
c) цікавість;
d) конкурентна боротьба;
e) прагнення самоствердитись за будь-яку ціну;
f) аварійні ситуації через стихійні лиха і вимкнення електроживлення;
g) відмови й збої апаратури;
h) помилки у програмному забезпеченні;
i) помилки в роботі персоналу;
j) перешкоди в лініях зв'язку через дії зовнішнього середовища.

1.16. Дії порушника можуть зумовлюватись такими мотивами:

a) незадоволеністю службовця кар'єрою;
b) хабаром;

c) цікавістю;
d) конкурентною боротьбою;
e) прагненням самоствердж уватися за будь-яку ціну;
f) аварійними ситуаціями через стихійні лиха і вимкнення електроживлення;
g) відмовами й збоями апаратури;
h) помилками у програмному забезпеченні;
i) помилками у роботі персоналу.

1.17. Можна скласти таку гіпотетичну модель потенційного порушника інформаційної безпеки:

a) кваліфікація порушника на рівні розробника системи;
b) порушник вибирає найсильнішу ланку в захисті;
c) порушником може бути стороння особа;
d) порушником може бути законний користувач системи;
e) порушником може бути власник інформації;
f) порушнику невідома інформація про принципи роботи системи;
g) порушник вибирає найслабшу ланку в захисті.

1.18. Навмисні дії, спрямовані на порушення інформаційної безпеки, можуть бути такі:

a) перехоплення;
b) розкрадання;
c) модифікація;
d) руйнування.

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

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

1.20. Заходи формування режиму інформаційної безпеки поділяють на такі рівні:

a) законодавчий (закони, нормативні акти, стандарти тощо);
b) морально-етичний (норми поведінки, недотримання яких спричинює зниження престижу конкретної людини або організації);

c) адміністративний (дії загального характеру, організації, що робляться керівництвом);
d) фізичний (механічні, електро- і електронно-механічні перешкоди на можливих шляхах проникнення потенційних порушників);
e) апаратний-програмний (електронні пристрої та спеціальні програми захисту інформації).

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

a) користувача "Admin" (для активізації діалогового вікна "Вхід");
b) користувача, що є власником бази даних і таблиць, які містяться в ній, запитів, форм, звітів і макросів;
c) будь-яких облікових записів користувача, доданих до групи "Admins".

1.22. Зазначте, чи можна використовувати символи « \ [].: | < > + =;,. ? * для паролів баз даних:

a) так;
b) ні.

1.23. Зазначте, чи забезпечується програмою Microsoft Access захист сторінок доступу до баз даних:

a) так;
b) ні.

1.24. Основними причинами пошкоджень електронної інформації за даними дослідницького центру DataPro Research є такі:

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.

1.25. Зазначте, що саме роблять зловмисники, дізнавшись інформації:

a) у 44 % випадків викрадають гроші з електронних рахунків;
b) у 14 % випадків викрадають гроші з електронних рахунків;
c) у 16 % випадків виводять з ладу програмне забезпечення;
d) у 46 % випадків виводять з ладу програмне забезпечення;
e) у 12 % випадків фальсифікують інформацію;
f) у 92 % випадків фальсифікують інформацію;
g) у 10 % випадків замовляють послуги, до яких не повинні мати доступу;
h) у 80 % випадків замовляють послуги, до яких не повинні мати доступу.

1.26. Конфіденційність інформації — це гарантія того, що:

a) конкретна інформація доступна тільки колу осіб, для якого призначена; порушення цієї категорії називається розкраданням, або розкриттям, інформації;
b) інформація нині існує в початковому вигляді, тобто при її зберіганні або передаванні не було здійснено несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення;
c) джерелом інформації є особа, яка заявлена як її автор; порушення цієї категорії так само називається фальсифікацією, але вже автора повідомлення.

1.27. Цілісність інформації — це гарантія того, що:

a) конкретна інформація доступна тільки колу осіб, для якого призначена; порушення цієї категорії називається розкраданням, або розкриттям, інформації;
b) інформація нині існує в початковому вигляді, тобто при її зберіганні або передаванні не було здійснено несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення;
c) джерелом інформації є особа, яка заявлена як її автор; порушення цієї категорії так само називається фальсифікацією, але вже автора повідомлення.

1.28. Автентичність інформації — це гарантія того, що:

a) конкретна інформація доступна тільки колу осіб, для якого призначена; порушення цієї категорії називається розкраданням, або розкриттям, інформації;

b) інформація нині існує в початковому вигляді, тобто при її зберіганні або передаванні не було здійснено несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення;
c) джерелом інформації є особа, яка заявлена як її автор; порушення цієї категорії так само називається фальсифікацією, але вже автора повідомлення.

1.29. Відносно інформаційних систем застосовуються такі категорії:

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

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

a) система поводиться в нормальному й позаштатному режимах так, як заплановано;
b) буде точно виконано команди;
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 цей момент до системи, є саме тим, за кого себе видає;
f) при умисному внесенні помилок у межах наперед обумовлених норм система поводитиметься так, як заплановано.

1.31. 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 здійснена повноцінна перевірка будь-якого компонента програмного комплексу;

d) клієнт, підключений у цей момент до системи, є саме тим, за кого себе видає;
e) при умисному внесенні помилок у межах наперед обумовлених норм система поводитиметься так, як заплановано.

1.32. Зазначте, яка з моделей абстрактного захисту інформації базується на теорії автоматів:

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

1.33. Зазначте, яка з моделей абстрактного захисту інформації базується на використанні трансакцій і ретельному оформленні прав доступу суб'єктів до об'єктів:

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

1.34. Зазначте, яка з моделей абстрактного захисту інформації базується на дослідженні поведінки множинних композицій функцій переходу з одного стану в інший:

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

1.35. До класу 0 належить така інформація:

a) недоступна у відкритому вигляді, але її розкриття не має жодної небезпеки;
b) загальнодоступна;
c) розкриття цієї інформації призведе до значних втрат на ринку;
d) розкриття цієї інформації призведе до фінансової загибелі компанії.

1.36. До класу 1 належить така інформація:

a) недоступна у відкритому вигляді, але її розкриття не має жодної небезпеки;
b) загальнодоступна;

c) розкриття цієї інформації призведе до значних втрат на ринку;
d) розкриття цієї інформації призведе до фінансової загибелі компанії.

1.37. До класу 2 належить така інформація:

a) недоступна у відкритому вигляді, але її розкриття не має жодної небезпеки;
b) загальнодоступна;
c) розкриття цієї інформації призведе до значних втрат на ринку;
d) розкриття цієї інформації призведе до фінансової загибелі компанії.

1.38. До класу 3 належить така інформація:

a) недоступна у відкритому вигляді, але її розкриття не має жодної небезпеки;
b) загальнодоступна;
c) розкриття цієї інформації призведе до значних втрат на ринку;
d) розкриття цієї інформації призведе до фінансової загибелі компанії.

1.39. 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 шляхом 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 таким штрафом:

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

здійснювати певну діяльність на термін до п'яти років, або виправними роботами на термін до двох років.

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

a) до сімдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на термін до двох років, або обмеженням волі на той самий термін;
b) від п'ятдесяти до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на термін до двох років;
c) до п'ятдесяти неоподатковуваних мінімумів доходів громадян або позбавленням права обіймати певні посади чи здійснювати певну діяльність на термін до п'яти років, або виправними роботами на термін до двох років.

1.41. Порушення правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж персоною, 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 таким штрафом:

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

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

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

1.43. Зазначте сферу використання програми Windows Disk Wiper:

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

1.44. Зазначте, в якій операційній системі паролі можуть зберігатися у вигляді малозначних контрольних сум (хеш-значень):

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

1.45. У момент відправлення пакету підтвердження або відкидання пароля в системі повинна бути встановлена така затримка:

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

1.46. Основні методи боротьби з копіюванням паролів такі:

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

1.47. Зазначте, в якій операційній системі паролі можуть зберігатись як у відкритому текстовому вигляді:

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

1.48. Зазначте, в якій операційній системі паролі можуть зберігатись у вигляді малозначних контрольних сум (хеш-значень):

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

1.49. Зазначте, які дані перевіряються на етапі аналізу таблиці ризиків:

a) визначається середньоквадратичне відхилення ризику;
b) перевіряється кожний рядок таблиці на неперевищення ризику визначеного значення;
c) порівнюється подвоєне значення з інтегральним ризиком;
d) визначається середньоарифметичне значення ризику.

1.50. Зазначте, на яких рівнях OSI (Open Systems Interconnection) проводиться атака на сервери:

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

1.51. Термінали захищеної інформаційної системи – це:

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

1.52. При використанні терміналів із фізичним доступом необхідно дотримувати таких вимог:

a) захищеність термінала повинна відповідати захищеності приміщення: термінали без пароля можуть бути тільки у приміщеннях, куди мають доступ особи відповідного або вищого рівня доступу. Відсутність імені реєстрації можлива тільки тоді, коли до термінала має доступ тільки одна людина, або якщо на групу осіб, що мають до нього доступ, поширюються загальні заходи відповідальності; термінали, встановлені в публічних місцях, завжди повинні запрошувати ім'я реєстрації й пароль;
b) системи контролю за доступом у приміщення зі встановленим терміналом повинні працювати повноцінно і згідно із загальною схемою доступу до інформації;
c) у разі встановлення термінала в місцях із широким скупченням народу клавіатура, а за потреби й дисплей, повинні бути обладнані пристроями, що дозволяють бачити їх тільки працюючому в цей момент клієнту (непрозорі скляні або пластмасові огорожі, шторки, "втоплена" модель клавіатури).

Номер теми	Назва розділу, теми курсу	Зміст завдання	Форма контролю
1	2	3	4
Модуль ІІ. Системи шифрування інформації			
1	Класифікація крипто-алгоритмів	1. Тайнопис, криптографія з ключем. 2. Симетричні та асиметричні криптоалгоритми	Конспект

Закінчення таблиці

2	Крипто-графічні засоби шифрування інформації	1. Квадрат полібія. Мережа фейштеля. Шифрування заміною (підстановкою), перестановкою, маршрути гамільтона, гаміювання аналітичних перетворень, комбіновані методи. 2. Стандарт DES (Data Encryption Standard). Приклад дешифрування	Конспект
3	Практичне шифрування інформації	1. Приклад кодування інформаційних послідовностей скремблером 1012 із початковим ключем 1102. 2. Коди криптоалгоритмів мовою програмування PASCAL. 3. Хеширування паролів. Алгоритм “Tandem DM”. Алгоритм Диффи-Хеллмана	Конспект
4	Системи шифрування даних, які передаються в мережах	1. Канальне шифрування. 2. Абонементне шифрування. 3. Стандарт блокових шифрів AES. Алгоритм RSA. 4. Блоковий шифр TEA	Конспект
Реферат			

ТЕМИ РЕФЕРАТІВ

1. Криптоалгоритми.

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

2. Системи шифрування даних у мережах.

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

3. Управління ключами.

Література [11; 14; 15; 24; 30; 34]

4. Аутинтифікація та ідентифікація.

Література [1; 3; 5]

5. Скремблери.

Література [1; 7; 11]

6. Мережа Фейштеля.

Література [1; 7; 11]

7. Перестановчі, підстановчі криптоалгоритми.

Література [2; 5; 11; 14; 15; 24]

8. Системи шифрування дискових даних.

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

9. Стратегія захисту інформації у фінансово-економічних інформаційних системах.

Література [1–8; 12; 13; 19; 22–24; 26; 42]

10. Класична модель симетричної системи секретного зв'язку за К. Шенноном.

Література [11; 14; 24; 30; 34]

11. Числові алгоритми в симетричній та асиметричній криптографії.

Література [2; 5; 24; 30; 34]

12. Системи прозорого шифрування.

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

13. Системи спеціальних видів шифрування.

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

14. Система симетричного шифрування.

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

15. Система асиметричного шифрування.

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

16. Стратегія захисту інформації в банківських інформаційних системах.

Література [1–8; 12; 13; 19; 22–24; 26; 42]

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ТА ДИСКУСІЇ

1. Визначення поняття "елементарні шифри".
2. Системи шифрування даних, які передаються в мережах (канальне та абонементне шифрування).
3. Загальна ідея односторонньої функції з лазівкою.
4. Засоби управління криптографічними ключами: генерація зберігання і розподіл ключів.
5. Політика ролей. Технології цифрових підписів.
6. Системи аутентифікації електронних даних (імітовставка, електронний підпис).
7. Класифікація криптоалгоритмів.
8. Тайнопис, криптографія з ключем, симетричні та асиметричні криптоалгоритми. Скремблери.

9. Стратегія захисту інформації у фінансово-економічних інформаційних системах.
10. Мережа Фейштеля.
11. Класична модель симетричної системи секретного зв'язку за К. Шенноном.
12. Криптографічні протоколи.
13. Числові алгоритми в симетричній та асиметричній криптографії.
14. Перестановчі, підстановчі криптоалгоритми.
15. Поточні, блочні шифри. Одиниці кодування.
16. Системи шифрування дискових даних (системи прозорого та спеціального видів шифрування).
17. Призначення програми Super File Encryption. Порядок шифрування та дешифрування файлів у програмі Super File Encryption. Порядок підбору параметрів шифрування та дешифрування файлів.
18. Призначення утиліти (T-CEC Pro). Порядок шифрування, дешифрування файлів утилітою (T-CEC Pro).
19. 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.

Тести

1. Апаратно-програмні засоби захисту інформації поділяються на такі групи:

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

2.2. Для реалізації імітовставки використовується принцип:

a) симетричного шифрування;
b) асиметричного шифрування.

2.3. Для реалізації електронного підпису використовується принцип:

a) симетричного шифрування;
b) асиметричного шифрування.

2.4. Традиційними вважаються системи, що базуються на таких типах даних:

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

2.5. Біометричними вважаються системи, що базуються на таких типах даних:

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

2.6. Зазначте, які алгоритми шифрування використовує програма BestCrypt:

a) Blowfish;
b) Twofish;
c) ГОСТ 28147–89.

2.7. Алгоритм Blowfish розробив:

a) Брюс Шнеїр разом із Джоном Келсеєм, Крісом Холом, Нілсом Фергузоном, Девідом Уогнером і Дугом Вітінгом;
b) Джоан Даємен і Вінсент Риджмен;
c) Брюс Шнеїр.

2.8. Алгоритм Twofish розробив:

a) Брюс Шнеїр разом із Джоном Келсеєм, Крісом Холом, Нілсом Фергузоном, Девідом Уогнером і Дугом Вітінгом;
b) Джоан Даємен і Вінсент Риджмен;
c) Брюс Шнеїр.

2.9. Зазначте, яка з програм може використовувати контейнер для шифрування:

a) Super File Encryption;

b) T-CEC Pro;
c) BestCrypt.

2.10. Ідея дешифрування шифру типу "Скитала" належить:

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

2.11. Криптографія — це:

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

2.12. Криптоаналіз — це:

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

2.13. При оцінці ефективності шифру зазвичай керуються правилом:

a) Аристотеля;
b) Керкхоффа;
c) Курчатова;
d) Лейбниця.

2.14. Зазначте, які алфавіти шифрування використовуються в сучасних ІС:

a) Z33 — 32 букви російського алфавіту і пропуск;
b) Z256 — символи, що входять у стандартні коди ASCII і КОИ-8;
c) бінарний — Z2 = {0,1};
d) вісімковий або шістнадцятковий.

2.15. Алгоритм RSA створили:

a) Райвест, Шамір і Адлеман (розкладання великих чисел на прості множники);
b) Діффі й Хелман (обчислення логарифма або піднесення у ступінь).

2.16. Алгоритм DH створили:

a) Райвест, Шамір і Адлеман (розкладання великих чисел на прості множники);
b) Діффі й Хелман (обчислення логарифма або піднесення у ступінь).

2.17. Алгоритм DES використовує ключ завдовжки:

a) 56 біт;
b) 256 біт.

2.18. Алгоритм ГОСТ 28147-89 використовує ключ завдовжки:

a) 56 біт;
b) 256 біт.

2.19. Скремблерами називаються:

a) перетворення блоку вхідної інформації фіксованої довжини й одержання результуючого блоку такого самого об'єму, але недоступного для прочитання сторонніми персонами, що не мають ключа;
b) програмні або апаратні реалізації алгоритму, що дають змогу шифрувати побітно безперервні потоки інформації.

2.20. Усі сучасні криптосистеми мають в основі такі шифри:

a) блокові;
b) потокові.

2.21. Блоковими є такі алгоритми:

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

2.22. Сучасні методи захисних перетворень поділяються на такі групи:

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

МЕТОДИЧНІ ВКАЗІВКИ ДО ПІДГОТОВКИ, НАПИСАННЯ ТА ЗАХИСТУ РЕФЕРАТУ

Реферат є складовою вивчення дисципліни.

Завдання підготовлені відповідно до курсу "Комп'ютерна безпека" для спеціалістів.

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

Оформлення й захист рефератів повинні сприяти активному засвоєнню нового матеріалу, формуванню вміння комплексного використання суміжних дисциплін при вирішенні практичних питань.

Структура реферату

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

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

Виконання та оформлення реферату

У рефераті розкривають історичні передумови проблеми, відповідають на теоретичні питання, наводять опис технології розв'язання практичного завдання, якщо це передбачено рефератом.

Відповіді на теоретичні питання потребують ретельної роботи з літературними джерелами. З конспектування літературних джерел роблять висновки. У тексті реферату потрібно давати посилання на

використану літературу. У висновках розглядають питання економічної доцільності та практичного застосування сучасних інформаційних технологій і обчислювальної техніки в галузі захисту.

Реферат слід оформлювати на стандартних аркушах паперу, зброшурованих у папку. Усі сторінки мають бути пронумеровані. 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 подають розрахунок варіанта реферату та питання. На останній сторінці студент підписує роботу і ставить дату. Роботу вкладають у файл з дискетою, де наведені текст, графічні матеріали.

Вибір варіанта реферату

Кожний студент отримує окреме завдання згідно з варіантом, що обчислюється за формулою

$$Z = \mathrm{mod}_{16}\,(NZK + PR - 2000) + 1,$$

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

Наприклад, якщо NZK = 398, PR = 2001, то

$Z = \mathrm{mod}_{16}(398 + 2001 - 2000) + 1 = \mathrm{mod}_{16}(399) + 1 = 15 + 1 = 16.$

Отже, Z = 16.

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 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.

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 практ. 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 практ. занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 70 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. — 502 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”).
7. *Касперский Е.* “Дыры” в MS-DOS и программы защиты информации // КомпьютерПресс. — 1991. — № 10.
8. *Теоретические* основы информационной безопасности (Дополнительные главы): Учеб. пособие / А. П. Баранов, Д. П. Зегжда, П. Д. Зегжда и др. — СПб., 1998. — 174 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. — 286 с.
17. *Зегжда Д. П., Корт С. С., Каулио В. В.* Теоретические основы информационной безопасности: Руководство к практ. занятиям / Под ред. П. Д. Зегжды. — СПб., 1998. — 34 с.
18. *Защита* информации в компьютерных системах: Лаборатор. практикум / П. Д. Зегжда, Д. Ю. Копылов, С. С. Корт и др.; Под ред. П. Д. Зегжды. — СПб., 1996. — 90 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. П. Д. Зегжды. — СПб., 1998. — 74 с.
26. *Перший А. Ю.* Организация защиты вычислительных систем // КомпьютерПресс. — 1992. — № 10–11. — С. 33–50.
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. П. Д. Зегжды. — СПб., 1998. — 48 с.
31. *Защита* информации в персональных компьютерах / А. В. Спесивцев и др. — М.: Радио и связь, 1992.
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.
35. *Уайт Д.* Электромагнитная совместимость радиоэлектронных средств и непреднамеренные помехи: Пер. с англ. — М.: Сов. радио, 1979. — 464 с. — Вып. 3.
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. — 106 с.
43. *Закон* України “Про інформацію”.
44. *Закон* України “Про інформацію в автоматизованих системах”.
45. *Закон* України “Про науково-технічну інформацію”.
46. *Закон* України “Про державну таємницю”.
47. http://www.dstszi.gov.ua — Сайт департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України.

ЗМІСТ

Відповідальний за випуск *А. Д. Вегеренко*
Редактор *А. А. Карпова*
Комп'ютерне верстання *М. М. Соколовська*

Зам. № ВКЦ-3030
Міжрегіональна Академія управління персоналом (МАУП)
03039 Київ-39, вул. Фрометівська, 2, МАУП