МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

НАВЧАЛЬНА ПРОГРАМА
дисципліни
“КОМП’ЮТЕРНА БЕЗПЕКА (БЕЗПЕКА ПРОГРАМ ТА ДАНИХ)”
(для спеціалістів)

Київ
ДП «Видавничий дім «Персонал»
2012

Підготовлено доцентом кафедри інформатики та інформаційних технологій, кандидатом технічних наук *В. М. Ахрамовичем*

Затверджена на засіданні кафедри інформатики та інформаційних технологій МАУП (протокол № 21 від 23.04. 08)

Перезатверджено на засіданні кафедри прикладної математики та інформаційних технологій (протокол № 33 від 13.07.11)

Схвалено Вченою радою Міжрегіональної Академії управління персоналом

Ахрамович В. М. Навчальна програма дисципліни "Комп'ютерна безпека (Безпека програм та даних)" (для спеціалістів). — К.: ДП «Вид. дім «Персонал», 2012. — 18 с.

Навчальна програма містить пояснювальну записку, тематичний план та зміст дисципліни "Комп'ютерна безпека (Безпека програм та даних)", рекомендації до виконання контрольної роботи, варіанти контрольних робіт, питання для самоконтролю, а також список літератури.

ЗМІСТ

Відповідальний за випуск *А. Д. Вегеренко*
Редактор *С. М. Толкачева*
Комп’ютерне верстання *А. А. Кучерук, О. М. Бабаєва*

Зам. № ВКЦ-4075

Формат 60×84/16. Папір офсетний.
Друк ротаційний трафаретний.

Ум. друк. арк. 1,05. Обл.-вид. арк. 0,88 . Наклад 30 пр.

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

ДП «Видавничий дім «Персонал»

03039 Київ-39, просп. Червонозоряний, 119, літ. ХХ

Свідоцтво про внесення до Державного реєстру суб’єктів видавничої справи ДК № 3262 від 26.08.2008

Надруковано в друкарні ДП «Видавничий дім «Персонал»

ПОЯСНЮВАЛЬНА ЗАПИСКА

Сучасне суспільство для задоволення своїх потреб вимагає забезпечення надійного захисту інформації. Особливої гостроти вона набуває у зв’язку з масовою комп’ютеризацією всіх видів діяльності людини, при об’єднанні ЕОМ у мережі та підключення до корпоративних та глобальних мереж. Тому для спеціалістів різноманітного профілю актуальною є підготовка в галузі захисту інформації. Саме для такої підготовки й призначена дисципліна “Комп’ютерна безпека”. Результатом вивчення дисципліни є засвоєння сучасних технологій захисту інформації та отримання практичних навичок організації ефективної системи безпеки комп’ютерних систем і мереж.

Вибір серед багатьох сучасних методів і засобів захисту таких, що найбільше відповідають конкретним умовам діяльності та забезпечують достатній рівень безпеки, є достатньо складним завданням, особливо для початківців. Разом з тим, багато технологій захисту мають чимало спільних рис у розробці і використанні. Це дає можливість вивчати сучасні технології на прикладах, що, незважаючи на новизну, вже стали класичними. Такими вибрано технології застосування захисту операційної системи, мережевих екранів, криптографічних систем, систем визначення атак і реакцій на атаку, систем моніторингу інформаційної безпеки. Вивчення цих технологій спирається на ґрунтовну теоретичну базу та аналіз вітчизняних і закордонних нормативних документів у галузі захисту інформації.

Сучасна інформаційна система є складною системою, з великою кількістю компонентів різного ступеня автономності, які зв’язані між собою й обмінюються даними. Практично кожен компонент може піддатися зовнішній дії або вийти з ладу. Компоненти автоматизованої інформаційної системи можна розбити на наступні групи:

- апаратні засоби — комп’ютери і їх складові (процесори, монітори, термінали, периферійні пристрої — дисководи, принтери, контролери, кабелі, лінії зв’язку тощо);
- програмне забезпечення — придбані програми, результатні, об’єктні, завантажувальні модулі; операційні системи і системні програми (компілятори, компонувальники та ін.), утиліти, діагностичні програми тощо;
- дані — що зберігаються тимчасово й постійно, на магнітних носіях, друкарські, архіви, системні журнали тощо.

Небезпечні дії на комп'ютерну інформаційну систему можна підрозділити на випадкові і навмисні. Аналіз досвіду проектування, виготовлення й експлуатації інформаційних систем показує, що інформація піддається різним випадковим діям на всіх етапах циклу життя системи.

Міждисциплінарні зв'язки: курс ґрунтується на знаннях, отриманих студентами в курсах "Інформатика та комп'ютерна техніка", "Архітектура комп'ютерів", "Інтернет та інтернет-технології", "Технології і засоби адміністрування комп'ютерних мереж", "Методи та засоби комп'ютерних інформаційних технологій", "Технологія програмування та створення програмних продуктів" тощо. Вивчення дисципліни буде сприяти кращому розумінню предмета при опануванні наступних навчальних дисциплін: "Організація баз даних та баз знань", "Програмне забезпечення автоматизованих систем", "Використання пакетів прикладних програм"та ін.

Мета вивчення дисципліни:

1. Оволодіння студентами комплексом знань у галузі захисту інформації, системами й методами визначення захищеності програмних продуктів, пристроїв; комп'ютерних мереж, їх складових та набуття на основі цих знань практичних навичок та 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 галузі захисту: операційних систем, текстових редакторів, табличних процесорів, систем управління базами даних, конфіденціальної інформації тощо. Набуття на основі вказаних знань практичних навичок, необхідних для розробки систем захисту, керування розробкою систем захисту, а на основі вказаного, нормального забезпечення роботи фінансових організацій, регіонів країни зі збереженням характеристик трафіку, швидкості санкціонованого доступу тощо.
3. Опанування концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденціальних документів; стратегією вибору систем виявлення атак, навичками роботи з пристроями безпеки в локальних та глобальних

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. —ТИИЭР. — Т. 76. — № 5.
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.: Связь,1980.
37. *Хорев А. А.* Способы и средства защиты информации. — М.: МОРФ, 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. рек. —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.

практ. // Под ред. проф. П. Д. Зегжды. — Изд. СПбГТУ, 1996. — 89 с.
19. *Касперський 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 практич. 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., Мэдник С.* Защита ЭВМ. — М.: Мир,1982.

комп’ютерних мережах із метою використання їх, можливостей для покращання показників безпеки в них.

У результаті вивчення навчальної дисципліни “Комп’ютерна безпека” 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, в 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 та глобальних комп’ютерних мережах банків та інших фінансових установ, на основі вивчених алгоритмів вміти розробляти нові програмні складові захисту в майбутньому;
- здобути практичні навички роботи з концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденціальних документів; роботи з системами й методами визначення захищеності носіїв інформації; створення засобами стандартного програмного забезпечення елементів захисту інформації; формулювати завдання щодо питань захисту інформації та, формалізуючи їх, вказувати шляхи вирішення.

ТЕМАТИЧНИЙ ПЛАН
дисципліни
“КОМП’ЮТЕРНА БЕЗПЕКА”

№ пор.	Назва змістового модуля і теми
	Змістовий модуль І. Основні положення теорії захисту інформації
1	Категорії інформаційної безпеки
2	Визначення політики безпеки. Абстрактні моделі захисту інформації
3	Законодавча база в галузі захисту інформації
	Змістовий модуль ІІ. Безпека інформаційних систем
4	Класи безпеки. Критерії інформаційної безпеки. Канали витоку інформації
5	Класифікація криптоалгоритмів
6	Системи шифрування даних, які передаються в мережах
7	Сучасна ситуація у галузі інформаційної безпеки. Рівні мережевих атак
8	Апаратні та програмні засоби захисту інформації в мережах
9	Термінали захищеної інформаційної системи. Отримання пароля на основі помилок
Разом годин: 54	

ЗМІСТ
дисципліни
“КОМП’ЮТЕРНА БЕЗПЕКА (БЕЗПЕКА ПРОГРАМ ТА ДАНИХ)”

Змістовий модуль І. Основні положення теорії захисту інформації

Тема 1. Категорії інформаційної безпеки

Основні визначення і поняття теорії захисту інформації. Технічний та програмний захист інформації.

Історія розвитку. Сфера застосування. Термінологія.

Література [1; 3–5; 8; 10; 36; 40; 41]

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. — С. 9 (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. *Баранов А. П., Зегжда Д. П., Зегжда П. Д., Ивашко А. М., Корт С. С.* Теоретические основы информационной системы: Учеб. пособие. — СПб., 1998. — 173 с.
9. *В. Жельников.* Криптография от папируса до компьютера. — М.: ABF, 1996.
10. *Галатенко В. А., Гагин А. В.* Информационная безопасность — обзор основных положений (часть 1, 2, 3) // Jet INFO. — 1996. — № 1–3.
11. *Герасименко В. А., Размахнин М. К.* Криптографические методы в автоматизированных системах // Зарубеж. радиоэлектроника. — 1982. — № 8.
12. *Головкин Б. А.* Надежное программное обеспечение // 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. — Т. 76. — № 5. — С. 24–42.
15. *Джефф П. Р.* Шифрование данных методом гаммирования // Электроника. — 1973. — Т. 46. — № 1.
16. *Защита* программного обеспечения / Пер. с англ. Д. Гроувер, Р. Сатер, Дж. Фипс и др. // Под ред. Д. Гроувера — М.: Мир, 1992. — 285 с.
17. *Зегжда Д. П., Корт С. С., Каулио В. В.* Теоретические основы информационной безопасности: Руководство к практ. занятиям// Под ред. проф. П. Д. Зегжды. — СПб., 1998 г. — 34 с.
18. *Зегжда П. Д., Копылов Д. Ю., Корт С. С., Медведовский И. Д.* и др. Защита информации в компьютерных системах: Лаборатор.

41. Засоби управління криптографічними ключами: генерація, зберігання і розподілення ключів.
42. Канали витоку інформації.
43. Що таке мережевий екран та його основні функції?
44. Наведіть перелік типових компонентів мережевих екранів.
45. Які ви знаєте обмеження функціонування мережі, пов'язані з використанням брандмауерів?
46. Класифікація мережевих екранів.
47. Поясніть типову політику використання мережевих екранів.
48. Наведіть коротку характеристику популярних брандмауерів.
49. Рівні мережевих атак (фізичний, канальний, мережевий, транспортний, сеансовий) відповідно до моделі OSI.
50. Типи атак.
51. Політика ролей. Технології цифрових підписів.
52. Стратегія вибору систем виявлення атак.
53. Системи аутентифікації електронних даних (імітовставка, електронний підпис).
54. Класифікація криптоалгоритмів.
55. Тайнопис, криптографія з ключем, симетричні та асиметричні криптоалгоритми. Скремблери.
56. Мережа Фейштеля.
57. Перестановні, підстановні криптоалгоритми.
58. Поточні, блочні шифри. Одиниці кодування.
59. Системи шифрування дискових даних (системи прозорого та спеціального видів шифрування).
60. Термінали захищеної інформаційної системи.

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 практическим занятиям. — СПб., 1998 — 128 стр.
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 г. — 69 стр.

Тема 2. Визначення політики безпеки. Абстрактні моделі захисту інформації

Абстрактні моделі та формальні моделі захисту інформації. Особливості моделей Белла-Ла Падуяі та Біба.

Література [1; 3–5; 8; 10; 36; 40; 41]

Тема 3. Законодавча база в галузі захисту інформації

Закони України "Про інформацію", "Про захист інформації в автоматизованих системах".

Вимоги вітчизняних стандартів захисту конфіденційної інформації від несанкціонованого доступу під час обробки в автоматизованих системах.

Зарубіжна нормативна база в галузі технічного захисту інформації. "Оранжева книга" безпеки. Критерії, вимоги та категорії систем безпеки "Оранжевої книги".

Література [1–8; 12; 13; 16–23; 25–27; 29; 33; 37–42]

Змістовий модуль II. Безпека інформаційних систем

Тема 4. Класи безпеки. Критерії інформаційної безпеки. Канали витоку інформації

Класи безпеки інформації та інформаційних систем. Класифікація систем за критеріями інформаційної безпеки.

Вимоги стосовно роботи з конфіденційною інформацією.

Створення політики інформаційної безпеки. Електромагнітні та електричні канали витоку інформації. Параметричні канали витоку інформації.

Література [1; 3–5; 8; 10; 22; 25–27; 35; 36; 40–42]

Тема 5. Класифікація криптоалгоритмів

Тайнопис, криптографія з ключем. Симетричні та асиметричні криптоалгоритми.

Література [4; 5; 11; 14; 15; 30; 34]

Тема 6. Системи шифрування даних, які передаються в мережах

Канальне шифрування. Абонементне шифрування.

Література [4; 5; 11; 14; 15; 30; 34]

Тема 7. Сучасна ситуація у галузі інформаційної безпеки. Рівні мережевих атак

Рівні мережевих атак відповідно до моделі OSI. Захист систем передавання інформації.

Література [1–8; 12; 13; 16–23; 25–27; 29; 33; 37–42]

Тема 8. Апаратні та програмні засоби захисту інформації в мережах

Системи ідентифікації й аутентифікації користувача (традиційні та біометричні параметри).

Система FireWall-1/VPN-1. Система OmniGuard/Enterprise Security Manager компанії Axent. Брандмауери, мережевий екран PIX Firewall.

Апаратно-програмний комплекс захисту інформації "ШИП", "Dallas Lock". Криптографічний адаптер. Процесор безпеки мережі. Локатори ліній зв'язку.

Сканер NetRecon. Аналізатор телефоних ліній SP-18/T "Багер-01".

Детектор електромагнітного поля Д-006.

Література [1–8; 12; 13; 16–23; 25–27; 29; 33; 37–42]

Тема 9. Термінали захищеної інформаційної системи. Отримання пароля на основі помилок

Термінали захищеної інформаційної системи. Отримання пароля на основі помилок адміністратора та користувача. Отримання пароля на основі помилок у реалізації. Соціальна психологія й інші способи отримання пароля.

Література [1–8; 12; 13; 16–23; 25–27; 29; 33; 37–42]

РЕКОМЕНДАЦІЇ ДО ВИКОНАННЯ КОНТРОЛЬНОЇ РОБОТИ

Контрольна робота є складовою вивчення дисципліни.

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

Мета — допомогти студентам засвоїти теоретичні знання, розвивати і удосконалювати навички, необхідні для створення подання, обробки, виконання професійних функцій з використанням сучасних програмних та апаратних засобів для захисту інформації.

Структуру контрольної роботи наведено в таблиці.

16. Класи безпеки.
17. Критерії інформаційної безпеки.
18. Стратегія захисту інформації у фінансово-економічних інформаційних системах.
19. Комплекс технічних та програмних засобів захисту інформації.
20. Сучасна ситуація в галузі інформаційної безпеки.
21. Класифікація інформації за рівнем конфіденційності.
22. Вимоги при роботі з конфіденційною інформацією.
23. Створення дерева каталогів із правами доступу. Зміна змісту каталогу access. conf.
24. Добавлення користувача та встановлення його прав.
25. Яким чином можливо використати помилку "переповнення буферу" для атаки на комп'ютерну систему?
26. Основні компоненти комплексної системи захисту інформації.
27. Наведіть перелік і поясніть зміст критеріїв оцінки рівня; безпеки інформації.
28. Наведіть перелік типових механізмів захисту інформації.
29. Як можна запобігти спробі несанкціонованого копіювання прикладної програми з компакт-диску?
30. Як можна запобігти спробі несанкціонованого копіювання прикладної програми з дискети?
31. Як можна запобігти спробі несанкціонованого копіювання текстової інформації?
32. Як здійснюється захист програм від вивчення?
33. Як здійснюється аналіз програмних реалізацій?
34. Поясніть спільні риси та відмінності зовнішніх атак на комп'ютерну систему від атак "зсередини"?
35. Що таке програма типу "троянський кінь"?
36. Навіщо використовуються та як реалізовані програми фальшивої реєстрації?
37. Як здійснюється аутентифікація користувачів за допомогою одноразових паролів?
38. Як здійснюється аутентифікація користувачів за допомогою фізичних об'єктів?
39. Як здійснюється аутентифікація користувачів за допомогою біометричних даних?
40. Системи шифрування даних, які передаються в мережах (канальне та абонементне шифрування).

Варіант 9

1. Відповідальність за протиправні дії згідно із законодавством України.
2. Які обмеження функціонування мережі, пов'язані з використанням брандмауерів ви знаєте?
3. Побудова моделі захисту системи, визначення затрат часу, ресурсів та засобів.

Варіант 10

1. Як здійснюється аутентифікація користувачів за допомогою біометричних даних?
2. Системи шифрування дискових даних (системи прозорого та спеціального видів шифрування).
3. Отримання пароля на основі помилок у реалізації. Соціальна психологія та інші способи отримання пароля.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Наведіть перелік загроз інформації.
2. Що таке загроза цілісності даних?
3. Що таке загроза доступності інформації?
4. Що таке загроза несанкціонованого доступу до даних?
5. Які сучасні моделі захищених інформаційних систем ви знаєте?
6. Поясніть зміст моделі захисту Белла-Ла Падулі.
7. Поясніть зміст моделі захисту Біба.
8. Зміст політики безпеки захищеної системи.
9. Відповідальність за протиправні дії згідно із законодавством України.
10. Основні положення Закону України "Про захист інформації в автоматизованих системах" щодо організації захисту інформації.
11. Загальні вимоги щодо захисту інформації відповідно до Закону України "Про захист інформації в автоматизованих системах".
12. Категорії інформаційної безпеки з точки зору інформації та інформаційних систем.
13. Технічні, програмно-апаратні та адміністративні засоби захисту інформації.
14. Визначення об'єкта захисту та можливих загроз.
15. Ідентифікація й аутентифікація. Механізми підзвітності та аудиту.

Орієнтовна структура і обсяги контрольної роботи

План (розділи)	Обсяг у сторінках (приблизно)	Короткий зміст (що потрібно з'ясувати)
Вступ	До однієї	Мета, загальна характеристика, визначення номера варіанта завдання
Назва кожного питання відповідно до теми реферату	1 — 2, загальний обсяг роботи в межах 20–30	Викладення суті питання з наведенням прикладів та посилань на літературні джерела
Висновки	До однієї	Прикладне значення
Список літератури	До однієї	
Додатки	До трьох	Якщо є

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

Виконання та оформлення контрольної роботи.

Студент повинен виконати реферат, в якому розкрити історичні посилання цієї проблеми, відповісти на всі питання теоретичного характеру, описати технологію розв'язання практичного завдання, якщо це передбачено рефератом.

Відповідь на теоретичні питання потребує ретельної роботи з літературою. Крім виписок і конспектування з літературних джерел, наприклад, із Internet, студент має зробити висновки. Робота повинна виконуватися самостійно. В тексті реферату потрібно давати посилання на використану літературу. У висновках розглядають питання економічної доцільності і практичного застосування сучасних інформаційних технологій та обчислювальної техніки у галузі захисту.

Реферат оформлюють на стандартних аркушах паперу, зброшурованих у папку. Усі аркуші пронумеровують. На титульній сторінці необхідно вказати назву вищого навчального закладу, факультет,

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

На першій сторінці повинні бути подані розрахунок варіанта контрольної роботи та питання варіанта і проставлені номери сторінок, на яких викладено цей матеріал. На останній сторінці студент підписує роботу і ставить дату. У кінці роботи необхідно подати список використаної літератури. Зшиту папку вкладають у поліетиленовий файл, де має бути дискета з повним текстом, графікою тощо набраного варіанта реферату.

Вибір варіанта контрольної роботи:

кожний студент отримує окреме завдання для виконання контрольної роботи згідно з варіантом Z, що обчислюється за формулою:

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

де NZK — номер залікової книжки (студентського квитка);

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 тут $Z=10$.

Зауваження

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

Увага!

Неправильно оформлена робота без перевірки повертається на доопрацювання. Роботу, виконану не за своїм варіантом, треба переробити.

ВАРІАНТИ КОНТРОЛЬНОЇ РОБОТИ

Варіант 1

1. Наведіть перелік загроз інформації.
2. Створення дерева каталогів із правами доступу. Зміна змісту каталогу access. conf.
3. Як розрахувати необхідний рівень захисту програмного продукту від несанкціонованого використання?

Варіант 2

1. Стратегія захисту інформації у фінансово-економічних інформаційних системах.
2. Поясніть спільні риси та відмінності зовнішніх атак на комп'ютерну систему від атак "зсередини".
3. Політика ролей. Технології цифрових підписів.

Варіант 3

1. Технічні, програмно-апаратні та адміністративні засоби захисту інформації.
2. Як можна запобігти спробі несанкціонованого копіювання прикладної програми з компакт-диску?
3. Що таке мережевий екран та його основні функції?

Варіант 4

1. Критерії інформаційної безпеки.
2. Класифікація криптоалгоритмів.
3. Поясніть модель оптимізації режиму моніторингу систем інформаційної безпеки.

Варіант 5

1. Які сучасні моделі захищених інформаційних систем ви знаєте?
2. Комплекс технічних та програмних засобів захисту інформації.
3. Перестановні, підстановні криптоалгоритми.

Варіант 6

1. Ідентифікація й аутентифікація. Механізми підзвітності та аудиту.
2. Системи шифрування даних, які передаються в мережах (канальне та абонементне шифрування).
3. Установлення та зміна паролів, контроль доступу в систему, права користувачів.

Варіант 7

1. Як здійснюється аутентифікація користувачів за допомогою фізичних об'єктів?
2. Типи атак.
3. Служби, які можуть захищати від кібероблав.

Варіант 8

1. Зміст політики безпеки захищеної системи.
2. Засоби управління криптографічними ключами: генерація, зберігання і розподілення ключів.
3. Мережа Фейштеля.