ЗМІСТ

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

Зам. № ВКЦ-4086

Формат 60×84/16. Папір офсетний.
Друк ротаційний трафаретний. Ум. друк. арк. 0,9. Обл.-вид. арк. 0,7.
Наклад 50 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 р.

Надруковано в друкарні ДП «Видавничий дім «Персонал»

МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

НАВЧАЛЬНА ПРОГРАМА
дисципліни
“ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ”
(для спеціалістів)

Київ
ДП «Видавничий дім «Персонал»
2012

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

Затверджено на засіданні кафедри інформатики та інформаційних технологій (протокол № 21 від 23.04.08)

Перезатверджено на засіданні кафедри прикладної математики та інформаційних технологій (протокол № 46 від 13.07.11)

Схвалено Вченою радою Міжрегіональної Академії управління персоналом

Ахрамович В. М. Навчальна програма дисципліни "Технології захисту інформації" (для спеціалістів). — К.: ДП «Вид. дім «Персонал», 2012. — 16 с.

Навчальна програма містить пояснювальну записку, тематичний план, зміст дисципліни "Технології захисту інформації", варіанти контрольних робіт, питання для самоконтролю, а також список літератури.

25. *Медведовский И. Д., Безгачев В. А., Юреленков А. П.* Информационная безопасность распределенных вычислительных систем: Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 73 с.
26. *Перший А. Ю.* Организация защиты вычислительных систем // 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 практическим занятиям / Под ред. проф. П. Д Зегжды. — СПб., 1998. — 47 с.
31. *Спесивцев А. В.* и др. Защита информации в персональных компьютерах. — М.: Радио и связь. 1992. — С. 140–149.
32. *Сяо Д., Керр Д., Мэдник С.* Защита ЭВМ. — М.: Мир,1982.
33. *Тимофеев Ю. А.* Комплексный подход к защите коммерческой информации (почему и как надо защищать компьютерную систему) // Защита информации. — 1992. — № 1.
34. *Диффи У.* Первые десять лет криптографии с открытым ключом / ТИИЭР. — М.: Мир, 1988. — Т. 76, № 5, Май. — С. 54–74.
35. *Уайт Д.* Электромагнитная совместимость радиоэлектронных средств и непреднамеренные помехи: Вып. 3: Пер. с англ. — М.: Сов. радио, 1979. — 464 с.
36. *Уолкер Б. Дж., Блейк Я. Ф.* Безопасность ЭВМ и организация их защиты. — М.: Связь,1980.
37. *Хорев А. А.* Способы и средства защиты информации. — М.: МО РФ, 1998. — 316 с.
38. *Хоффман Л. Дж.* Современные методы защиты информации. — М.: Сов. радио, 1980.
39. *Щербаков А.* Построение программных средств защиты от копирования: Практические 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.

9. *Мельников 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, № 1, 2, 3, 1996.
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. *Дж. Л. Месси.* Введение в современную криптологию // ТИИЭР. — М.: Мир, 1988. — Т. 76, № 5, Май. — С. 24–42.
15. *Джефф П. Р.* Шифрование данных методом гаммирования // Электроника. — 1973. — Т. 46. — № 1.
16. *Защита* программного обеспечения / Д. Гроувер, Р. Сатер, Дж. Фипс и др. / Под ред. Д. Гроувера: Пер. с англ. — М.: Мир, 1992. — 285 с.
17. *Зегжда Д. П., Корт С. С., Каулио В. В.* Теоретические основы информационной безопасности: Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 34 с.
18. *Защита* информации в компьютерных системах: Лабораторный практикум / П. Д. Зегжда, Д. Ю. Копылов, С. С. Корт, И. Д. Медведовский и др.; Под ред. проф. П. Д. Зегжды. — СПб., 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.

ПОЯСНЮВАЛЬНА ЗАПИСКА

У сучасних умовах інформація, яка забезпечує життєво й історично важливі напрями діяльності людини, перетворюється в цінний продукт і основний товар, вартість якого поступово наближається до вартості продуктів матеріального виробництва, що робить її (інформацію) об'єктом інтересів різного характеру (комерційного, соціального, кримінального та ін.). Одним словом, виникнення індустрії обробки інформації привело до необхідності розвитку індустрії засобів захисту інформації.

Об'єктами посягань можуть бути технічні засоби (комп'ютери і периферія) як матеріальні об'єкти, програмне забезпечення і бази даних, для яких технічні засоби є оточенням.

У цьому сенсі комп'ютер може бути як предметом посягань, так й інструментом. Можливе об'єднання зазначених понять, коли комп'ютер одночасно і інструмент, і предмет. Зокрема, до цієї ситуації належить факт розкрадання машинної інформації, видалення її, порушення нормального процесу функціонування ЕОМ і мереж. Якщо це пов'язане із втратою матеріальних і фінансових цінностей, то цей факт можна кваліфікувати як злочин. Також якщо із цим фактом пов'язуються порушення інтересів національної безпеки, авторства, то кримінальна відповідальність прямо передбачена відповідно до законів України.

Особливу тривогу викликає те, що організовані злочинні формування активно використовують здобутки інформатики для досягнення злочинних цілей. Аналіз наявної емпіричної бази світового досвіду показує, що спостерігається тенденція, коли транснаціональна організована комп'ютерна злочинність становить загрозу не тільки національній безпеці окремої країни, а й загрожує всьому світовому порядку. Це стосується сфери економічної безпеки. Світовий "кіберпростір" у галузі економічних відносин активно освоюється криміналітетом. За експертними оцінками, обсяги операцій при електронній обробці та передаванні через комп'ютерні мережі грошових ресурсів вказують на те, що потенційні втрати можуть бути вищі, ніж при тих самих операціях з використанням звичайних паперових технологій. Втрати ж окремо взятої держави в таких випадках за лічені хвилини можуть досягати значних розмірів.

Міждисциплінарні зв'язки. Пропонований курс ґрунтується на знаннях, отриманих студентами при вивченні таких дисциплін, як

“Інформатика та комп’ютерна техніка”, “Архітектура комп’ютерів”, “Інтернет та інтранет технології”, “Технології і засоби адміністрування комп’ютерних мереж”, “Методи та засоби комп’ютерних інформаційних технологій”, “Технологія програмування та створення програмних продуктів”, “Організація баз даних та баз знань”, “Програмне забезпечення автоматизованих систем“, “Використання пакетів прикладних програм”та ін.

У результаті 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; про керівні документи, що визначають рівень захищеності комп’ютерних систем; про методи проведення аналізу надійності системи захисту інформації в комп’ютерних системах; про 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; про алгоритми кодування та застосування стандартного програмного забезпечення захисту; про методи та технологію захисту операційних систем, текстових редакторів, табличних процесорів, системи управління базами даних в локальних, корпоративних та 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, розподілу, обробки, використання та зберігання конфіденціальних документів; з системами й методами визначення захищеності носіїв інформації; створення засобами стандартного програмного забезпечення елементів захисту інформації; формулювання завдань з питань захисту інформації та визначення шляхів їх вирішення.

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

Передбачено постійний контроль у процесі вивчення дисципліни (захист лабораторних робіт, опитування на лекціях) та періодичний

46. Створення дерева каталогів із правами доступу. Зміна змісту каталогу access.conf.
47. Добавлення користувача та встановлення його прав.
48. Служби, які можуть захищати від кибероблав.
49. Установлення та зміна паролів, контроль доступу в систему, права користувачів.
50. Завдання моніторингу систем інформаційної безпеки.
51. Поясніть модель оптимізації режиму моніторингу систем інформаційної безпеки.
52. Критерії оптимізації режиму моніторингу систем інформаційної безпеки.
53. Як розрахувати необхідний рівень захисту програмного продукту від несанкціонованого використання?

СПИСОК ЛІТЕРАТУРИ

Основна

1. *Домарев В. В.* Безопасность информационных технологий. — СПб.: DiaSoft, 2002. — 688 с.
2. *Защита* компьютерных систем от разрушающих программных воздействий: Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 128 с.
3. *Зегжда Д. П., Калинин М. О., Степанов П. Г.* Теоретические основы информационной безопасности. Защищенные операционные системы: Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 69 с.
4. *Конев И., Беляев А.* Информационная безопасность предприятия. — СПб.: БХВ Петербург, 2003. — 752 с.
5. *Методы* и средства защиты информации / Под ред. Ю. С. Ковтанюка. — К.: ЮНИОР, 2003. — 501 с.

Додаткова

6. *О вирусах*, червях, троянцах и бомбах. Защита информации. Переводы. — М.: Знание, 1990. — (Новое в жизни, науке и технике. Сер. “Вычислительная техника и ее применение”). — С. 9.
7. *Касперський 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 безопасности (Дополнительные главы): Учеб. пособие. — СПб., 1998. — 173 с.

13. Канали витоку інформації.
14. Класифікація інформації за рівнем конфіденційності.
15. Класифікація криптоалгоритмів.
16. Тайнопис, криптографія з ключем.
17. Симетричні криптоалгоритми.
18. Асиметричні криптоалгоритми.
19. Скремблери.
20. Мережа Фейштеля.
21. Переставні криптоалгоритми.
22. Підставні криптоалгоритми.
23. Поточні, блочні шифри. Одиниці кодування.
24. Системи шифрування дискових даних (системи прозорого та спеціального видів шифрування).
25. Системи шифрування даних, які передаються в мережах (канальне та абонементне шифрування).
26. Системи аутентифікації електронних даних: імітовставка.
27. Системи аутентифікації електронних даних: електронний підпис.
28. Засоби управління криптографічними ключами: генерація, зберігання і розподілення ключів.
29. Стратегія захисту інформації у фінансово-економічних інформаційних системах.
30. Комплекс технічних засобів захисту інформації.
31. Комплекс програмних засобів захисту інформації.
32. Сучасна ситуація у сфері інформаційної безпеки.
33. Рівні мережних атак (фізичний, канальний) згідно із моделлю OSI.
34. Рівні мережних атак (мережний, транспортний, сеансовий) згідно із моделлю OSI.
35. Типи атак.
36. Вимоги при роботі з конфіденційною інформацією.
37. Політика ролей.
38. Технології цифрових підписів.
39. Стратегія вибору систем виявлення атак.
40. Термінали захищеної інформаційної системи.
41. Отримання пароля на основі помилок адміністратора та користувача.
42. Отримання пароля на основі помилок у реалізації.
43. Соціальна психологія й інші способи отримання пароля.
44. Побудова моделі захисту системи, визначення затрат часу, ресурсів та засобів.
45. Система пошуку та захисту від вторгнення LIDS.

контроль (контроль знань за кожним модулем, періодичні тестування, іспит з дисципліни).

ТЕМАТИЧНИЙ ПЛАН
дисципліни
“ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ”

№ пор.	Назва змістового модуля і теми
	Змістовий модуль І. Менеджмент інформаційної безпеки
1	Категорії інформаційної безпеки з точки зору інформації та інформаційних систем
2	Абстрактні моделі захисту інформації. Огляд найпоширеніших методів “злому”
3	Класи безпеки. Критерії інформаційної безпеки. Канали витоку інформації
4	Класифікація криптоалгоритмів
5	Системи шифрування даних, які передаються в мережах
6	Засоби управління криптографічними ключами
	Змістовий модуль ІІ. Менеджмент безпеки інформаційних систем
7	Сучасна ситуація у сфері інформаційної безпеки. Рівні мережних атак
8	Апаратні та програмні засоби захисту інформації в мережах
9	Термінали захищеної інформаційної системи. Отримання пароля на основі помилок
Разом годин: 162	

ЗМІСТ
дисципліни
“ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ”

Змістовий модуль І. Менеджмент інформаційної безпеки

Тема 1. Категорії інформаційної безпеки з точки зору інформації та інформаційних систем

Етапи розвитку систем захисту. Основні загрози інформаційній безпеці.

Категорії безпеки інформації та інформаційних систем.

“Помаранчева книга” США.

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

Тема 2. Абстрактні моделі захисту інформації. Огляд найпоширеніших методів “злому”

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

Огляд найпоширеніших методів “злому”. Комплексний пошук можливих методів доступу.

Термінали захищеної інформаційної системи.

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

Тема 3. Класи безпеки. Критерії інформаційної безпеки. Канали витоку інформації

Класи безпеки інформації та інформаційних систем. Класифікація систем за критеріями інформаційної безпеки. Вимоги до 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 4. Класифікація криптоалгоритмів

Тайнопис, криптографія з ключем. Симетричні та асиметричні криптоалгоритми.

Література [4; 5; 11; 14; 15; 30; 34]

Варіант 7

1. Класи безпеки.
2. Засоби управління криптографічними ключами: генерація, зберігання і розподілення ключів.
3. Побудова моделі захисту системи, визначення затрат часу, ресурсів та засобів.

Варіант 8

1. Критерії інформаційної безпеки.
2. Рівні мережних атак (фізичний, канальний, мережний, транспортний, сеансовий) згідно із моделлю OSI.
3. Отримання пароля на основі помилок у реалізації. Соціальна психологія й інші способи отримання пароля.

Варіант 9

1. Канали витоку інформації.
2. Вимоги при роботі з конфіденційною інформацією.
3. Отримання пароля на основі помилок адміністратора та користувача.

Варіант 10

1. Класифікація інформації за рівнем конфіденційності.
2. Системи шифрування даних, які передаються в мережах (канальне та абонементне шифрування).
3. Термінали захищеної інформаційної системи.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Категорії інформаційної безпеки з точки зору інформації та інформаційних систем.
2. Технічні засоби захисту інформації.
3. Програмно-апаратні засоби захисту інформації.
4. Адміністративні засоби захисту інформації.
5. Визначення об’єкта захисту та можливих загроз.
6. Принцип розімкнутого управління захистом інформації.
7. Принцип зворотного зв’язку при захисті інформації.
8. Відповідальність за протиправні дії згідно із законодавством України.
9. Ідентифікація й аутентифікація.
10. Механізми підзвітності та аудиту.
11. Класи безпеки.
12. Критерії інформаційної безпеки.

ВАРІАНТИ КОНТРОЛЬНОЇ РОБОТИ

Варіант 1

1. Категорії інформаційної безпеки з точки зору інформації та інформаційних систем.
2. Класифікація криптоалгоритмів.
3. Стратегія захисту інформації у фінансово-економічних інформаційних системах.

Варіант 2

1. Технічні, програмно-апаратні та адміністративні засоби захисту інформації.
2. Комплекс технічних і програмних засобів захисту інформації.
3. Установлення та зміна паролів, контроль доступу в систему, права користувачів.

Варіант 3

1. Визначення об'єкта захисту та можливих загроз.
2. Системи аутентифікації електронних даних (імітовставка, електронний підпис).
3. Служби, які можуть захищати від кибероблав.

Варіант 4

1. Принцип розімкнутого управління, компенсації, зворотного зв'язку.
2. Системи шифрування дискових даних (системи прозорого та спеціального видів шифрування).
3. Додавання користувача та встановлення його прав.

Варіант 5

1. Сучасна ситуація у сфері інформаційної безпеки.
2. Відповідальність за протиправні дії згідно із законодавством України.
3. Створення дерева каталогів із правами доступу. Зміна змісту каталогу access.conf.

Варіант 6

1. Ідентифікація й аутентифікація. Механізми підзвітності та аудиту.
2. Типи атак.
3. Система пошуку та захисту від вторгнення LIDS.

Тема 5. Системи шифрування даних, які передаються в мережах

Канальне шифрування. Абонементне шифрування.

Література [4; 5; 11; 14; 15; 30; 34]

Тема 6. Засоби управління криптографічними ключами

Генерація ключів. Зберігання і розподілення ключів.

Література [4; 5; 11; 14; 15; 30; 34]

Змістовий модуль II. Менеджмент безпеки інформаційних систем

Тема 7. Сучасна ситуація у сфері інформаційної безпеки. Рівні мережних атак

Рівні мережних атак згідно із моделлю 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. Мережний екран PIX Firewall.

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

Сканер NetRecon. Аналізатор телефонних 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]

ЗАВДАННЯ ДЛЯ КОНТРОЛЬНОЇ РОБОТИ

Контрольна робота є складовою навчального процесу вивчення дисципліни.

Пропоновані завдання підготовлені відповідно до курсу "Технології захисту інформації" для бакалаврів.

Мета контрольної роботи — допомогти студентам засвоїти теоретичні знання, набути практичних навичок виконання професійних функцій, пов'язаних з використанням сучасних програмних та апаратних засобів для захисту інформації.

Структура контрольної роботи

План (розділи)	Обсяг сторінок	Короткий зміст (що потрібно висвітлити)
Вступ	До однієї	Мета, загальна характеристика, визначення номера варіанта завдання
Назва кожного питання відповідно до реферату	1–2, загальний обсяг роботи — у межах 20–30	Викладення суті питання з 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.

Контрольна робота виконується у вигляді реферату.

Виконання та оформлення контрольної роботи

Студент повинен розкрити історичні передумови проблеми, що розглядається, висвітлити теоретичні питання, описати технологію розв'язання практичного завдання, якщо це передбачено рефератом.

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

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

На першій сторінці має бути наведено розрахунок варіанта контрольної роботи та питання варіанта із зазначенням сторінок, на яких викладено відповіді на питання. На останній сторінці студент має поставити свій підпис і дату. Наприкінці роботи необхідно подати список використаної літератури. Зшита папка має бути вкладена в поліетиленовий файл та містити дискету з повним текстом, графіками тощо реферату.

Вибір варіанта контрольної роботи

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

$Z = \mathrm{mod}_{12}(NZK + PR - 2000) + 1,$

де NZK — номер залікової книжки (студентського квитка) студента;

PR — поточний рік отримання завдання.

Наприклад, NZK = 398, PR =2001, тоді

$Z = \mathrm{mod}_{12}(398+2001 - 2000)+1 = \mathrm{mod}_{12}(399) + 1 = 3+1=4.$

Отже, тут Z=4.

Зауваження

1. Обчислення варіанта має бути 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 виконанню за новим варіантом.