МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ „ЛЬВІВСЬКА ПОЛІТЕХНІКА”

МЕТОДИЧНІ ВКАЗІВКИ

ДЛЯ ВИКОНАННЯ КОНТРОЛЬНОЇ РОЗРАХУНКОВОЇ РОБОТИ

З ДИСЦИПЛІНИ:

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Львів - 2022

Пропоновані методичні вказівки призначені для виконання контрольної розрахункової роботи з дисципліни Технології захисту інформації. Вказані завдання повинні сформувати в студентів навички з впровадження основних принципів організації захисту даних, які знадобляться їм для вирішення інженерних завдань.

Укладач: Басюк Т. М., к.т.н., доцент кафедри ІСМ

Контрольна розрахункова робота

ВСТУП

Захист інформації перетворюється сьогодні на одну з найактуальніших задач внаслідок надзвичайно широкого розповсюдження як власне різноманітних систем обробки інформації, так і розширення локальних та глобальних комп'ютерних мереж, якими передаються величезні об'єми інформації державного, військового, комерційного, приватного характеру, власники якої часто були б категорично проти ознайомлення з нею сторонніх осіб. Проблема набуває особливої гостроти після прийняття урядом України закону про захист персональних даних, який зобов'язує зберігати та передавати персональні дані працівників лише у захищеному вигляді в інформаційних системах.

Не менш важливим завданням вважається широке впровадження інформаційних технологій у різні сфери людської діяльності в Україні: стрімке зростання обігу пластикових карток, введення електронних паспортів та медичних карт, студентських квитків та залікових книжок; зрештою все більше державних установ та приватних підприємств переходять на електронний документообіг, який до того ж, вимагає юридичної чинності підпису фізичної або юридичної особи. Розповсюдження таких технологій також, безперечно, вимагає добре поставленого захисту інформації.

Усі ці та багато інших задач покликані вирішувати різноманітні технології захисту інформації. З огляду на те, представлені методичні вказівки призначені для закріплення знань з дисципліни технології захисту інформації з метою їх застосування для вирішення інженерних задач.

Контрольна розрахункова робота

ВИМОГИ ДО НАПИСАННЯ КОНТРОЛЬНОЇ РОЗРАХУНКОВОЇ РОБОТИ

У ході виконання КРР студенти систематизують, закріплюють і поглиблюють отримані знання, вміння й навички. При виконанні КРР студент повинен продемонструвати здатності до таких видів діяльності, як:

- пошук необхідної інформації із заданої теми;
- вивчення й критичний аналіз отриманих матеріалів;
- вивчення програмних засобів захисту інформації та вбудованих механізмів захисту загальносистемного програмного забезпечення;
- систематизація й узагальнення наявної інформації;
- самостійне визначення шляхів вирішення поставлених завдань;
- оформлення рішення завдань у вигляді пояснювальної записки;
- отримання навиків при розробці систем забезпечення інформаційної безпеки;
- логічне обґрунтування й формулювання висновків, пропозицій та рекомендацій із отриманих результатів роботи.

Структура контрольної розрахункової роботи

Номер розділу	Назва	Опис	Рекомендована к-сть стор.
Титульний лист	–	–	1
Зміст	Зміст	–	1-2
Вступ	Вступ	Зазвичай, вступ пишеться після написання основної частини роботи та висновків. Головне призначення введення до курсової роботи - обґрунтувати вибір теми,	1

		сформулювати поставлені завдання, охарактеризувати інформаційну базу, відзначити обмеження теми та інші особливості роботи. Необхідно розуміти, що у вступі не розглядається її змістовна частина, оскільки він передує основній роботі, пояснює її призначення, спрямованість і особливості.	
Розділ 1	Теоретична частина. (Назва розділу згідно з варіантом)	В даному розділі здійснюється пошук та аналіз літературних джерел за теоретичною частиною згідно з варіантом. Його метою є написання відповідних теоретичних відомостей, які відображають поточний стан досліджуваних завдань та необхідність в їх подальшому дослідженні	8-10

Контрольна розрахункова робота

Розділ 2	Порівняльний аналіз та формулювання вимог	Даний розділ містить критичний порівняльний аналіз відомих аналогів (програм, методів, моделей, методик, підходів) систем захисту. При цьому виділяються їх переваги та недоліки на основі яких визначаються функції розроблюваної програми та здійснюється опис відповідних вимог до її реалізації. Склад вимог до системи, що включаються в даний розділ встановлюють залежно від виду, призначення, специфічних особливостей і умов функціонування конкретної системи та включають: - вимоги до структури та особливостей функціонування системи; - вимоги до чисельності й кваліфікації персоналу системи й режиму його роботи; - вимоги до надійності; - вимоги до захисту інформації від несанкціонованого доступу; - вимоги по збереження даних в процесі нештатних ситуацій та зовнішніх впливів; - вимоги по стандартизації й уніфікації.	10
Розділ 3	Практична реалізація	Відповідно до описаних вимог та завдання здійснюється програмна реалізація системи та наводяться контрольні приклади які підтверджують правильність	10

		прийнятих проектних рішень	
Висновки	Висновки	Містить короткий виклад головних проблем і положень, викладених в роботі. У висновку не може міститися нових моментів, які не розглянуті в основній частині роботи. Він не є продовженням тексту роботи, а являє собою короткі висновки з її змісту. Крім того в даному підрозділі можна описати отримані знання та навички під час виконання КРР.	1-2
Список використаної літератури	Список використаної літератури	Містить перелік літературних джерел, які застосовувались при написанні КРР та вміщені у відповідні номери посилань по тексту роботи.	1-2

Завдання до написання контрольної розрахункової роботи

РОЗДІЛ 1. ВИКЛАСТИ ТЕОРЕТИЧНІ ПОЛОЖЕННЯ ЗГІДНО ІЗ ТЕМОЮ.

1. Нормативні документи в галузі захисту інформації в Україні
2. Стандарти безпеки, які застосовуються в інформаційних технологіях
3. Захист авторських прав в глобальній мережі Інтернет
4. Проблеми безпеки сучасних корпоративних мереж
5. Основні фактори, які впливають на безпеку інформації в комп'ютерних системах
6. Основні принципи забезпечення інформаційної безпеки
7. Моделі безпеки комп'ютерних мереж
8. Ядра безпеки й надійна обчислювальна база комп'ютерних мереж
9. Принципи й архітектури безпеки комп'ютерних мереж
10. Принципи архітектури безпеки ISO та DOD.

Контрольна розрахункова робота

11. Ідентифікація й автентифікація користувачів. Методи, що знижують ризик загрози розшифрування паролів.
12. Керування ключами в комп'ютерних системах (Накопичення та розподілення ключів, алгоритм Діфі-Хеллмана)
13. Біометричні дані ідентифікації в комп'ютерних мережах
14. Безпека IP адресації та DNS системи
15. Конфронтація між IPsec-архітектурою та мережними екранами
16. Фільтруючі маршрутизатори та їх застосування для забезпечення безпеки
17. Packet-filtering firewall (Мережевий екран з фільтрацією пакетів).
18. Circuit-level gateway (Шлюз сеансового рівня).
19. Application-level gateways (Шлюз прикладного рівня)
20. Stateful inspection firewall (Мережевий екран експертного рівня)
21. Персональні та динамічні мережеві екрани
22. Схеми підключення мережевих екранів
23. Поняття демілітаризованої зони та способи її організації
24. Системи виявлення атак на комп'ютерну мережу
25. Віртуальні приватні мережі. Особливості функціонування.
26. Концепція побудови захищених віртуальних приватних мереж VPN
27. Функції й компоненти мережі VPN. Механізми тунелювання й інкапсуляції.
28. Класифікація VPN. Загальний огляд та способи організації
29. Класифікація VPN за рівнем моделі OSI.
30. Класифікація VPN по архітектурі технічного рішення.
31. Класифікація VPN по способі технічного рішення.
32. Технічні й економічні переваги впровадження технологій VPN у корпоративні мережі
33. Пасивні та активні методи впливу на комп'ютерну мережу

Контрольна розрахункова робота

34. Протидія пасивним і активним методам впливу
35. Мережні атаки, засновані на використанні багів у програмному забезпеченні.
36. Методи протидії загрозі прослуховування трафіку
37. Методи, що знижують ризик загрози розшифрування паролів
38. Методи виявлення утиліт Rootkits, мережних черв'яків та вірусів.
39. Способи створення безпека для електронної пошти
40. Методи шифрування із симетричним ключем (Системи підстановок, Системи одноразового використання, Системи шифрування Віженера)
41. Системи шифрування з відкритим ключем (Практична реалізація RSA, Криптосистеми на основі еліптичних рівнянь)
42. Система шифрування Плейфера. Система шифрування Хілла.
43. Проблеми й перспективи криптографічних систем (Використання блукаючих ключів, Шифрування, кодування й стиск інформації)
44. Захист інформації від несанкціонованого доступу методом криптоперетворень
45. Інформаційна безпека в безпровідній мережі Wi-Fi
46. Поширені злочини у сфері комп'ютерної безпеки
47. Безпека в десктопних операційних системах. Особливості налаштування
48. Безпека в мобільних операційних системах. Особливості налаштування
49. Комп'ютерні віруси та антивірусне програмне забезпечення. Алгоритми роботи Захист інформації в комп'ютерній мережі підприємства
50. Особливості макровірусів, способи поширення та основні алгоритми роботи

Контрольна розрахункова робота

51. Програмні закладки: типи, способи впровадження та захисту
52. Безпека комп'ютерних мереж на основі інфраструктури відкритих ключів (Public Key Infrastructure);
53. Програмні засоби для захисту інформації від фірми Cisco
54. Програмні засоби для захисту інформації від фірми Kerio
55. Програмно-апаратні засоби захисту інформаційних ресурсів від несанкціонованого використання та копіювання з допомогою електронних ключів
56. Поняття стеганографії та основні алгоритми роботи
57. Аналіз та порівняльна характеристика існуючих програмних засобів комп'ютерної стеганографії
58. Методи стегааналізу (знаходження наявності прихованих повідомлень в контейнерах) тенденції розвитку
59. Захист електронної пошти. Порівняльний аналіз відомих систем/підходів
60. Аналіз методів перехоплення паролів користувачів комп'ютерних систем та методів їм протидії
61. Порівняльний аналіз персональних брендмауерів
62. Математичні основи стандарту шифрування Даних DES
63. Математичні основи алгоритму AES. Історія алгоритму AES.
64. Алгоритм безпечного хешування SHA
65. Електронний бізнес і комерційні ризики. Огляд IOTP протоколу
66. Торговельні процедури ("trading exchanges") і безпека
67. Загальна характеристика й функції PAPI-інтерфейсу
68. Поняття електронного підпису (Цифрова сигнатура)
69. Алгоритм цифрового підпису Ель Гамаля (EGSA)
70. Захищені електронні транзакції й технологія 3D Secure
71. Протидія пасивним і активним методам впливу

Контрольна розрахункова робота

72. Мережні атаки, засновані на використанні багів у програмному забезпеченні.
73. Методи протидії загрозі прослуховування трафіку
74. Методи, що знижують ризик загрози розшифрування паролів
75. Методи виявлення утиліт Rootkits, мережних черв'яків та вірусів.
76. Способи створення безпека для електронної пошти
77. Методи шифрування із симетричним ключем (Системи підстановок, Системи одноразового використання, Системи шифрування Віженера)
78. Системи шифрування з відкритим ключем (Практична реалізація RSA, Криптосистеми на основі еліптичних рівнянь)
79. Система шифрування Плейфера. Система шифрування Хілла.
80. Проблеми й перспективи криптографічних систем (Використання блукаючих ключів, Шифрування, кодування й стиск інформації)
81. Захист інформації від несанкціонованого доступу методом криптоперетворень
82. Інформаційна безпека в безпровідній мережі Wi-Fi
83. Поширені злочини у сфері комп'ютерної безпеки
84. Безпека в десктопних операційних системах. Особливості налаштування
85. Безпека в мобільних операційних системах. Особливості налаштування
86. Комп'ютерні віруси та антивірусне програмне забезпечення. Алгоритми роботи Захист інформації в комп'ютерній мережі підприємства
87. Особливості макровірусів, способи поширення та основні алгоритми роботи

Контрольна розрахункова робота

88. Програмно-апаратні засоби захисту інформаційних ресурсів від несанкціонованого використання та копіювання з допомогою електронних ключів
89. Поняття стеганографії та основні алгоритми роботи
90. Аналіз та порівняльна характеристика існуючих програмних засобів комп'ютерної стеганографії

РОЗДІЛ 2. ПРОПОНОВАНІ ТЕМИ ДЛЯ ВИКОНАННЯ КРР

Студент може запропонувати свою тему, не зазначену в тематиці кафедри, але вона обов'язково повинна бути узгоджена з керівником. Студенту доцільно визначити коло своїх інтересів і виконувати розрахункову роботу по одній проблематиці, що дозволить поглибити і розширити його творчі можливості та більш повно підготуватися до виконання подальших робіт. В будь-якому випадку вибір теми роботи повинен бути обґрунтований і не носити випадкового характеру.

1. Розробка системи, для торгового центру, що використовує парольну автентифікацію з додатковими засобами адміністрування (мінімальний та максимальний термін дії пароля, наявність списку використовуваних паролів та перевірка їх надійності шляхом аналізу за принципом атаки за словником)
2. Розробка системи блокового шифрування з вибором алгоритму шифрування
3. Розробка системи, що програмно реалізує функції хешування SHA
4. Розробка системи, що здійснює взаємну автентифікацію (створює захищений сеанс зв‘язку) двох хостів мережі на основі протоколу CHAP

Контрольна розрахункова робота

5. Розробка системи шифрування/розшифрування з використання алгоритму IDEA
6. Розробка системи протоколювання подій, пов‘язаних з доступом різних додатків/користувачів до обраних інформаційних ресурсів (папкам, принтерам, розділам реєстру)
7. Розробка системи для приховання та видобування інформації в графічних файлах
8. Розробка системи шифрування/розшифрування в режимі електронної кодової книги ECB
9. Розробка системи для обміну інформацією між хост-комп‘ютерами із проведення автентифікації на основі моделі «рукостискання»
10. Розробка системи, що програмно реалізує функції хешування MD4
11. Розробка системи шифрування/розшифрування в режимі DESX
12. Розробка системи, що здійснює взаємну автентифікацію (створює захищений сеанс зв‘язку) двох хостів мережі на основі протоколу s/key authentication
13. Розробка системи, яка надає інформацію щодо списку користувачів, які мають право доступу до обраного інформаційного ресурсу (папки, принтера, розділу реєстра) з вказанням наявних у них прав доступу
14. Розробка системи двохфакторної автентифікації
15. Розробка системи шифрування/розшифрування з використання алгоритму E2
16. Розробка системи для приховання та видобування інформації в звукових файлах
17. Розробка захищеної поштової клієнтської програми з автоматичним отриманням ЕЦП під повідомленням та перевіркою його при отриманні повідомлення

Контрольна розрахункова робота

18. Розробка системи для автентифікації користувачів за їх «підписом» з допомогою маніпулятора миші
19. Розробка системи шифрування/розшифрування в режимі зворотного зв'язку по виходу (OFB)
20. Розробка системи, що програмно реалізує функції хешування MD5
21. Розробка системи, що здійснює взаємну автентифікацію (створює захищений сеанс зв‘язку) двох хостів мережі на основі протоколу SSL
22. Розробка системи, яка надає інформацію щодо списку інформаційних ресурсів до яких має доступ на читання/запис заданий користувач та отримання інформації щодо списку ресурсів до яких мають право на читання всі користувачі
23. Розробка системи обліку трафіку користувачів інтернету
24. Розробка системи шифрування/розшифрування в режимі AES
25. Розробка системи для приховання та видобування інформації у відео файлах
26. Розробка системи для автентифікації користувачів за їх «клавіатурним почерком»
27. Розробка системи, що програмно реалізує функції хешування RIPEMD.
28. Розробка системи одноразової автентифікації
29. Розробка системи шифрування/розшифрування з використання алгоритму Cast
30. Розробка системи шифрування/розшифрування в режимі зчеплення шифрованих блоків (CBC)
31. Розробка системи шифрування/розшифрування згідно з алгоритмом RSA.

Контрольна розрахункова робота

32. Розробка системи отримання та перевірки ЕЦП за алгоритмом Ель-Гамаля
33. Розробка системи аналізу надійності роботи веб-сервера
34. Розробка системи шифрування/розшифрування в режимі 3-DES
35. Розробка системи для приховання та видобування інформації в текстових файлах
36. Розробка захищеної поштової клієнтської програми з автоматичним шифруванням/розшифруванням повідомлень та/або приєднаних до них файлів
37. Розробка системи для автентифікації користувачів на основі їх здатності до запам‘ятовування інформації, що відображається на короткий термін та екрані відображення
38. Розробка системи шифрування/розшифрування з використання алгоритму FROG
39. Розробка системи, що здійснює аналіз та виявлення паролів користувачів, які не відповідають вимогам безпеки та наявні у відкритих «словниках паролів»
40. Розробка системи захисту від несанкціонованого копіювання з використанням технології електронного цифрового підпису
41. Розробка системи аналізу захищеності в мережі Інтернет
42. Розробка системи двофазної фіксації транзакцій в протоколі Microsoft
43. Розробка системи архівування та дублювання критичної інформації користувача
44. Розробка системи шифрування/розшифрування в режимі гамування
45. Розробка системи визначення та візуалізації логічної структури мережі

Контрольна розрахункова робота

46. Розробка системи шифрування/розшифрування в режимі зворотного зв’язку за шифротекстом (CFB)
47. Розробка системи аналізу поштового трафіку на предмет виявлення листів, що відповідають визначеним ознакам
48. Розробка системи шифрування/розшифрування з використання алгоритму TWOFISH
49. Розробка системи моделювання проведення електронних транзакцій з використанням протоколу 3D-SECURE
50. Розробка системи шифрування/розшифрування з використання алгоритму RC4
51. Розробка системи, для торгового центру, що використовує парольну автентифікацію з додатковими засобами адміністрування (мінімальний та максимальний термін дії пароля, наявність списку використовуваних паролів та перевірка їх надійності шляхом аналізу за принципом атаки за словником)
52. Розробка системи блокового шифрування з вибором алгоритму шифрування
53. Розробка системи, що програмно реалізує функції хешування SHA
54. Розробка системи, що здійснює взаємну автентифікацію (створює захищений сеанс зв‘язку) двох хостів мережі на основі протоколу CHAP
55. Розробка системи шифрування/розшифрування з використання алгоритму Idea
56. Розробка системи протоколювання подій, пов‘язаних з доступом різних додатків/користувачів до обраних інформаційних ресурсів (папкам, принтерам, розділам реєстру)
57. Розробка системи для приховання та видобування інформації в графічних файлах

58. Розробка системи шифрування/розшифрування в режимі електронної кодової книги ECB
59. Розробка системи для обміну інформацією між хост-комп‘ютерами із проведення автентифікації на основі моделі «рукостискання»
60. Розробка системи, що програмно реалізує функції хешування MD4
61. Розробка системи шифрування/розшифрування в режимі DESX
62. Розробка системи, що здійснює взаємну автентифікацію (створює захищений сеанс зв‘язку) двох хостів мережі на основі протоколу S/KEY AUTHENTICATION
63. Розробка системи, яка надає інформацію щодо списку користувачів, які мають право доступу до обраного інформаційного ресурсу (папки, принтера, розділу реєстра) з вказанням наявних у них прав доступу
64. Розробка системи двохфакторної автентифікації
65. Розробка системи шифрування/розшифрування з використання алгоритму e2
66. Розробка системи для приховання та видобування інформації в звукових файлах
67. Розробка захищеної поштової клієнтської програми з автоматичним отриманням ЕЦП під повідомленням та перевіркою його при отриманні повідомлення
68. Розробка системи для автентифікації користувачів за їх «підписом» з допомогою маніпулятора миші
69. Розробка системи шифрування/розшифрування в режимі зворотного зв'язку по виходу (OFB)
70. Розробка системи, що програмно реалізує функції хешування MD5
71. Розробка системи для обміну інформацією між хост-комп‘ютерами із проведення автентифікації на основі моделі «рукостискання»

72. Розробка системи, що програмно реалізує функції хешування MD4
73. Розробка системи шифрування/розшифрування в режимі DESX
74. Розробка системи, що здійснює взаємну автентифікацію (створює захищений сеанс зв‘язку) двох хостів мережі на основі протоколу s/key authentication
75. Розробка системи, яка надає інформацію щодо списку користувачів, які мають право доступу до обраного інформаційного ресурсу (папки, принтера, розділу реєстра) з вказанням наявних у них прав доступу
76. Розробка системи двохфакторної автентифікації
77. Розробка системи обліку трафіку користувачів інтернету
78. Розробка системи шифрування/розшифрування в режимі AES
79. Розробка системи для приховання та видобування інформації у відео файлах
80. Розробка системи для автентифікації користувачів за їх «клавіатурним почерком»
81. Розробка системи, що програмно реалізує функції хешування RIPEMD.
82. Розробка системи одноразової автентифікації
83. Розробка системи шифрування/розшифрування з використання алгоритму Cast
84. Розробка системи шифрування/розшифрування в режимі зчеплення шифрованих блоків (CBC)
85. Розробка системи аналізу захищеності в мережі Інтернет
86. Розробка системи двофазної фіксації транзакцій в протоколі Microsoft
87. Розробка системи архівування та дублювання критичної інформації користувача

Контрольна розрахункова робота

88. Розробка системи шифрування/розшифрування в режимі гамування
89. Розробка системи визначення та візуалізації логічної структури мережі
90. Розробка системи шифрування/розшифрування в режимі зворотного зв'язку за шифротекстом (CFB)

ОФОРМЛЕННЯ КРР

КРР представляється до захисту у вигляді зброшурованої пояснювальної записки та електронного носія. Електронний носій містить у собі всі розділи пояснювальної записки, графічні файли, створене програмне забезпечення (разом із ресурсними файлами). Виклад матеріалу в пояснювальній записці повинен бути коротким і точним. Пояснювальну записку друкують машинописним способом (текстовий редактор Microsoft Word):

Шрифт	Times New Roman
Розмір шрифту	14 пунктів
Відстань між рядками	1,5 інтервали
Параметри сторінки	Формат А4
Розташування	Книжкове
Поля документу	20 мм

Заголовки структурних частин пояснювальної записки "ЗМІСТ", "ВСТУП", "РОЗДІЛ", "ВИСНОВКИ", "СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ" друкують великими літерами симетрично до тексту. Заголовки підрозділів друкують маленькими літерами (крім першої великої) з абзацного підступу. Крапку в кінці заголовка не ставлять. Якщо заголовок складається з двох або більше речень, їх розділяють крапкою. Кожну структурну частину пояснювальної записки треба починати з нової сторінки. Нумерацію сторінок, розділів, підрозділів, пунктів, підпунктів,

малюнків, таблиць, формул подають арабськими цифрами без знака №.

Першою сторінкою є титульний аркуш, який включають до загальної нумерації сторінок. На титульному аркуші номер сторінки не ставлять, на наступних сторінках номер проставляють посередині внизу сторінки. Зміст, вступ, висновки, список використаних джерел не мають порядкового номера, але всі аркуші, на яких розміщені згадані структурні частини, нумерують звичайним чином. Не нумерують лише їх заголовки, тобто не можна друкувати "1.ВСТУП", або "Розділ 4. ВИСНОВКИ".

Ілюстрації (фотографії, креслення, схеми, графіки, карти) і таблиці необхідно подавати безпосередньо після тексту, де вони згадані вперше, або на наступній сторінці. Ілюстрації позначають словом "Рис." і нумерують послідовно в межах розділу. Номер ілюстрації повинен складатися з номера розділу і порядкового номера ілюстрації, між якими ставиться крапка. Наприклад: Рис. 1.2 (другий рисунок першого розділу).

При написанні КРР студент повинен здійснювати посилання на джерела, матеріали або окремі результати з яких наводяться в пояснювальній записці. Посилання в тексті на джерела слід зазначати порядковим номером за переліком посилань, виділеним двома квадратними дужками, наприклад, "... у працях [1-7]...".

Список використаних джерел розміщують в абетковому порядку прізвищ перших авторів. Відомості про джерела, включені до списку, необхідно давати відповідно до вимог державного стандарту з обов’язковим наведенням назв праць.

ЗРАЗОК ТИТУЛЬНОГО ЛИСТА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ „ЛЬВІВСЬКА ПОЛІТЕХНІКА”

кафедра
інформаційних систем
та мереж

Контрольна розрахункова робота
з дисципліни %%
Варіант %

Виконав (Виконала)
студент (студентка)
групи %%-%%
Прізвище та ініціали студента
Прийняв (Прийняла)
Посада
Прізвище та ініціали викладача

Львів-202%

ЛІТЕРАТУРА

1. Анин Б. Защита компьютерной информации /Б.Анин – СПб.: БХВ, 2009. – 384с.
2. Белов Е. Б. Основы информационной безопасности. Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р. В. Мещеряков, А. А. Шелупанов – М.: Горячая линия - Телеком, 2006. – 544 с.
3. Биячуев Т.А. Безопасность корпоративных сетей / Т.А. Биячуев – СПб.: ИТМО, 2014. – 161 с.
4. Богуш В.М. Інформаційна безпека: термінологічний навчальний довідник / В.М. Богуш, В.Г. Кривуца, А.М. Кудін – К.: Д.В.К., 2010. – 508 с.
5. Домарёв В. В. Защита информации и безопасность компьютерных систем / В. В. Домарёв – К.: Diasoft, 2009. – 453с.
6. Дорошенко А. Н. Информационная безопасность. Методы и средства защиты информации в компьютерных системах : учебн. пособ. / А. Н. Дорошенко, Л. Л. Ткачев. – М. : МГУПИ, 2006. – 143 с.
7. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – Введ. 01.01.98. – К. : Держстандарт України, 1997. – 11 с.
8. ДСТУ 4145–2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – К. : Держстандарт України, 2002. – 40 с.
9. Зима В. Безопасность глобальных сетевых технологий / В. Зима, А. Молдовян, Н. Молдовян. – СПб.: БХВ, 2012. – 368 с.
10. Кавун С.В. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.
11. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 512с.
12. Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников – М.: Финансы и статистика, 2007. – 368с.
13. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
14. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер ; пер. с англ. – М. : Изд. ТРИУМФ, 2002. – 816 с.