Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та управління

Кафедра інформаційної та кібернетичної безпеки

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ О.Б.Жильцов
«_14_» ___09_____ 2018 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ЗАХИСТ ІНФОРМАЦІЇ»

для студентів

галузі знань	0403 Системні науки та кібернетика
напряму підготовки	6.040302 Інформатика
освітнього рівня	першого (бакалаврського)

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 09/4/18
(підпис) (прізвище, ініціали)
«___» _____ 2018 р.

Київ – 2018

Розробник:

Рой Яніна Володимирівна, кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Викладач:

Рой Яніна Володимирівна, кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки

Протокол від 13.09.2018 р. № 6

Завідувач кафедри _____ В.Л. Бурячок
(підпис)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 122 Інформатика)

___.___. 20___ р.

Керівник освітньої програми _____ І.В. Машкіна
(підпис)

Робочу програму перевірено

___.___. 20___ р.

Заступник директора/декана _____ І.Ю. Мельник
(підпис)

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	4	
Семестр	7	
Кількість змістових модулів з розподілом:	3	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	42	
Модульний контроль	6	
Семестровий контроль	30	
Самостійна робота	42	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Захист інформації» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів другого (магістерського) рівня відповідно до навчального плану спеціальності 6.040302 Інформатика 012.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Захист інформації» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Захист інформації» складається з трьох змістових модулів: Основні поняття захисту інформації, Безпека і захист даних, Криптографічний захист інформації. Обсяг дисципліни – 120 год (4 кредити).

Метою викладання навчальної дисципліни «Захист інформації» є вивчення основних методів та засобів захисту інформаційних ресурсів, які реалізовані у сучасних базових технологіях інформаційної безпеки.

Завдання:

- вивчення теоретичних основ і положень захисту інформації;
- вивчення способів криптографічного перетворення інформації;
- отримання необхідних теоретичних знань побудови систем захисту інформації;
- отримання практичних навиків адміністрування систем захисту інформації

У результаті вивчення навчальної дисципліни формуються загальні компетентності:

- ***компетентності у сфері навчання:***
  - здатність до організації самостійної навчальної, практичної та науково-дослідної діяльності;
- ***компетентності у сфері застосування знань в практичних ситуаціях***
  - вміння застосовувати здобуті теоретико-концептуальні професійні знання у

процесі практичної, викладацької та науково-дослідної роботи;

фахові компетентності:

- ***компетентності у сфері інформаційної безпеки:***
  - здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки;
  - здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;.
  - здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності;
  - здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки.
- **компетентності у сфері науково-дослідної діяльності:**
  - уміння вивчати і систематизувати досягнення вітчизняних і зарубіжних досліджень у галузі інформаційно-комунікаційних технологій, педагогіки і психології, суміжних галузей знань;
  - вивчати, узагальнювати й упроваджувати на практиці вітчизняний і зарубіжний досвід управління інформаційними технологіями і системами, інформаційною інфраструктурою тощо.
- **компетентності у сфері вмінь працювати в групі:**
  - здатність використовувати навички взаємодії в роботі, компетентності у сфері навичок міжособистісного спілкування
  - здатність до продуктивного використання комунікації як складової професійної діяльності.

3. Результати навчання за дисципліною

При вивченні курсу «Захист інформації» студенти повинні

знати:

– основні міжнародні і національні положення та стандарти з безпеки в інформаційно-телекомунікаційних системах;

– технології забезпечення конфіденціальності інформаційних систем;

– технології забезпечення автентичності інформаційних систем;

– технології забезпечення цілісності даних інформаційних систем;

– методи та процедури цифрової стеганографії;

уміти:

– забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації;

– забезпечувати захист програмного та інформаційного забезпечення від несанкціонованих дій;

– розробляти й вирішувати актуальні питання теорії і практики інформаційної безпеки;

– застосовувати знання в практичній діяльності.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Основні поняття захисту інформації							
Тема 1. Інформаційні системи та технології як об’єкти інформаційної безпеки	7	2					5
Тема 2. Основи безпеки інформаційних ресурсів	6	2			2		2
Тема 3. Організаційний та правовий захист інформації	4	2			2		
Тема 4. Основи інженерно-технічного захисту інформації	9	2			2		5
Модульний контроль	2						
Разом	28	8			6		12
Змістовий модуль 2. Безпека і захист даних							
Тема 1. Механізми і політики розмежування прав доступ	9	2			2		5
Тема 2. Методи та пристрої забезпечення захисту і безпеки	4	2			2		
Тема 3 Захист, доступ та автентифікація	1**1**	2			4		5
Модульний контроль	2						
Разом	26	6			8		10
Змістовий модуль 3. Криптографічний захист інформації							
Тема 1. Основні напрями розвитку сучасної криптографії	9	2			2		5
Тема 2. Механізми та протоколи керування ключами	9	2			2		5
Тема 3 Шифрування даних	1**6**	2			4		1**0**
Модульний контроль	2						
Разом	3**6**	6			8		2**0**
Підготовка та проходження контрольних заходів	30						
Усього	12**0**	20			22		42

5. Програма навчальної дисципліни

Змістовий модуль 1. Основні поняття захисту інформації.
Основні питання:

- Інформаційні системи та технології як об’єкти інформаційної безпеки
- Основи безпеки інформаційних ресурсів
- Організаційний та правовий захист інформації
- Основи інженерно-технічного захисту інформації

Змістовий модуль 2. Безпека і захист даних

Основні питання:

- Механізми і політики розмежування прав доступ
- Методи та пристрої забезпечення захисту і безпеки
- Захист, доступ та автентифікація

Змістовий модуль 3. Криптографічний захист інформації

Основні питання:

- Основні напрями розвитку сучасної криптографії
- Механізми та протоколи керування ключами
- Шифрування даних

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен.
- *Комп'ютерного контролю:* тестові програми.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Ма	Модуль 1	Модуль 2	Модуль 3

	максимальна кількість балів за одиницю	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	4	4	3	3	3	3
Відвідування семінарських занять	1						
Відвідування практичних занять	1						
Відвідування лабораторних занять	1	3	3	4	4	4	4
Робота на семінарському занятті	10						
Робота на практичному занятті	10						
Лабораторна робота (в тому числі допуск, виконання, захист)	10	3	30	4	40	4	40
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25
Виконання ІНДЗ	30						
Разом		-	67	-	77	-	77
Максимальна кількість балів: 191							
Розрахунок коефіцієнта: 191/60=3,18							

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
	Змістовий модуль 1. Основні поняття захисту інформації	12	5
1	Основи інженерно-технічного захисту інформації • виконання завдань відповідно до теми; • опрацювання фахових видань.	12	5
	Змістовий модуль 2. Безпека і захист даних	10	5

2	Аналіз методів і засобів несанкціонованого здобуття інформації по технічних каналах • виконання завдань відповідно до теми; • опрацювання фахових видань.	10	5
	Змістовий модуль 3. Криптографічний захист інформації	20	5
3	Дослідження сучасних блокових шифрів: • виконання завдань відповідно до теми; • опрацювання фахових видань.	20	5
	Разом	42	15

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп'ютерний тест, що складається 20 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – комбінована. Екзамен оцінюється у 40 балів за розподілом: 20 балів – комплексний комп'ютерний тест з дисципліни; 20 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями з побудови та управління ІТ-інфраструктурою навчального закладу.

Оцінювання практичного завдання відбувається в межах від 0 до 20 балів, згідно критеріїв оцінювання, й здійснюється з урахуванням: рівнів сформованості аналітико-синтетичних, творчих та методичних умінь необхідних для побудови ІТ-інфраструктури освітнього закладу.

Бали за виконання тесту та бали за виконання практичного завдання додаються. Оцінювання результатів засвоєння теоретичних знань та оцінювання сформованості практичних навичок володіння цифровими технологіями студентами, продемонстровані на екзамені, представлене у таблиці.

Підсумкова кількість балів (max – 40)	Оцінка за 4-бальною шкалою

1 – 23	«незадовільно»
24 – 29	«задовільно»
30 – 35	«добре»
36 – 40	«відмінно»

Орієнтовний перелік питань для екзамену

1. Аутентифікація й авторизація користувачів.
2. Домен захисту.
3. Аутентифікація користувачів за допомогою одноразових паролів.
4. Аутентифікація користувачів за допомогою фізичних об’єктів.
5. Аутентифікація користувачів за допомогою біометричних даних.
6. Основні компоненти системи захисту ОС Windows.
7. Захист файлової системи NTFS.
8. Основні компоненти системи захисту ОС Linux.
9. Основні компоненти системи захисту Web-серверу Apache.
10. Основні компоненти системи захисту Web-серверу IIS.
11. Програмний код для обмеження доступу до змісту Web-сторінки за допомогою пароля.
12. Типові заходи безпеки під час роботи з електронною поштою.
13. Особливості протоколу TCP/IP та їх використання в мережевих екранах.
14. Мережевий екран і його основні функції.
15. Типові компоненти мережевих екранів.
16. Обмеження функціонування мережі, пов’язані з використанням брандмауерів.
17. Класифікацію мережевих екранів.
18. Типова політика використання мережевих екранів.
19. Охарактеризуйте популярні брандмауери.
20. Криптографія та крипто аналіз.
21. Актуальність проблеми надійності діючих криптосистем.
22. Криптограма, криптосистема, ключ.
23. Зміст симетричної системи секретного зв’язку.
24. Поняття моделі супротивника, практичної стійкості шифроперетворення.
25. Проблема безпечного розповсюдження ключів у симетричних системах секретного зв’язку.
26. Одностороння функція з лазівкою.
27. Зміст асиметричної системи секретного зв’язку
28. Завдання, які виконуються за допомогою асиметричної системи секретного зв’язку.
29. Елементарні шифри.
30. Зміст поняття ключового потоку.
31. Основні типи шифрів.
32. Загальні алгоритмічні проблеми, пов’язані зі стійкістю сучасних крипто алгоритмів.
33. Цифровий підпис.
34. Криптографічні протоколи в асиметричних системах секретного зв’язку.
35. Принципи розробки систем визначення атак на комп’ютерну систему.
36. Принципи розробки систем реакції на атаку комп’ютерних систем.
37. Класифікація систем визначення атак на комп’ютерну систему.
38. Типові компоненти систем визначення атак на комп’ютерну систему.
39. Принципи функціонування систем визначення атак на комп’ютерну систему на базі методу визначення аномалій.
40. Принципи функціонування систем визначення атак на комп’ютерну систему на базі визначення зловживань.
41. Основні принципи функціонування систем реакцій на атаку.
42. Завдання моніторингу систем інформаційної безпеки.
43. Модель оптимізації режиму моніторингу систем інформаційної безпеки.

44. Критерії оптимізації режиму моніторингу систем інформаційної безпеки.
45. Особливості обчислення потрібного рівня захисту програмного продукту від несанкціонованого використання.
46. Запобіжні засоби спробі несанкціонованого копіювання прикладної програми з компакт-диску.
47. Запобіжні засоби спробі несанкціонованого копіювання прикладної програми з дискети
48. Запобіжні засоби спробі несанкціонованого копіювання текстової інформації
49. Реалізація захисту програм від вивчення
50. Аналіз програмних реалізацій
51. Концепції інформатизації суспільства.
52. Поняття теорії захисту інформації і загальна структура її науково-методологічної основи.
53. Моделі систем захисту і процесів захисту інформації. Системна класифікація моделей захисту. Узагальнена модель захисту інформації, її можливості.
54. Поняття про загрозу інформації. Види загроз і їхня системна класифікація.
55. Методи і моделі оцінки уразливості інформації. Уразливість інформації, конкретні типи уразливостей.
56. Методи оцінки параметрів інформації, що захищається. Методика визначення необхідного рівня захисту інформації. Функціональна й організаційна побудова СЗІ. Визначення і принципи побудови криптографічних СЗІ.
57. Визначення основних понять криптології. Класифікація атак на криптоалгоритми.
58. Шифрування методом гаммування.
59. Сучасні симетричні й асиметричні криптосистеми.
60. Принципи розсіювання, перемішування і переплутування. Складений шифр.
61. Основні способи шифрування. Потокові алгоритми шифрування. Їхні достоїнства і недоліки. Блокові алгоритми шифрування. Їхні достоїнства і недоліки.
62. Асиметричні криптосистеми. Приклад узагальненої схеми Диффі-Хеллмана.
63. Прийоми криптоаналізу. Алгоритм криптопротоколу для розподілу секретних сеансових ключів.
64. Суть специфічних криптопротоколів. Приклади протоколів з частковим поділом секрету.
65. Особливості захисту інформації в ЕОМ. Вимоги захисту інформації при захисті каналів передачі даних. Загрози інформації для персональних ЕОМ.
66. Ідентифікація і перевірка дійсності в комп'ютерних системах. Ідентифікація і механізми підтвердження дійсності користувача.
67. Електронний цифровий підпис.
68. Керування криптографічними ключами. Метод генерації ключів для симетричної криптосистеми. Модифікація ключів. Концепція ієрархії ключів. Проблема аутентифікації майстрів-ключів, захисту сеансових ключів.
69. Протокол SKIP управління криптоключами.
70. Аналіз програмних реалізацій. Динамічний метод аналізу програм. Етапи динамічного аналізу програм. Захист програм від вивчення.
71. Класи способів захисту від налагодження і дизасемблювання. Спосіб динамічного перетворення програми під час її виконання.
72. Захист від програмних впливів, що руйнують. Класи "шкідливих програм".
73. Принципами розумної достатності інформаційної безпеки мережі Internet.
74. Особливості побудови захищеної ОС у порівнянні з традиційними ОС мереж.
75. Особливості функціонування міжмережевих екранів.
76. Політики мережевої безпеки підприємства. Суть політики доступу до мережевих сервісів, її основні принципи.
77. Політика реалізації МЕ, принципи заснування правил доступу до внутрішніх ресурсів. Функціональні вимоги до компонентів МЕ.
78. Основні компоненти міжмережевих екранів.
79. Шлюз мережного рівня. Програмні методи захисту.

80. Можливі способи реалізації SKIP-захисту трафіка IP-пакетів.
81. Особливості безпеки мереж стосовно вилучених атак.
82. Поняття типової погрози безпеки.
83. Суть атаки "аналіз мережного трафіка".
84. Різновиди атак "підміна довіреного об'єкта або суб'єкта РВС".
85. Здійснення атаки "впровадження у РВС помилкового суб'єкта шляхом нав'язування помилкового маршруту".
86. Здійснення атаки "впровадження у РВС помилкового суб'єкта через недоліки алгоритмів пошуку".
87. Принципи функціонування електронних платіжних систем.
88. Види пластикових карт. Карти з пам'яттю і смарт-карты. Методи генерації значення PIN-номера.
89. Забезпечення безпеки систем POS і банкоматів.
90. Принципи побудови універсальної електронної платіжної системи UEPS

Шкала відповідності оцінок

Рейтингова оцінка	**Сума балів за всі види навчальної діяльності**	**Значення оцінки**
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов’язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов’язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов’язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 120 год., лекції – 20 год., лабораторні роботи – 22 год., модульний контроль – 6 год., самостійна робота –42 год., семестровий контроль – 30 год.

Модулі (назви, бали)	**Змістовий модуль 1. Основні поняття захисту інформації (67 балів)**				**Змістовий модуль 2. Безпека і захист даних (77 балів)**			**Змістовий модуль 3. Криптографічний захист інформації (77 балів)**		
Лекції (теми, бали)	Інформаційні системи та технології як об'єкти інформаційної безпеки (1 бал)	Основи безпеки інформаційних ресурсів (1 бал)	Організаційний та правовий захист інформації (1 бал)	Основи інженерно-технічного захисту інформації (1 бал)	Механізми і політики розмежування прав доступ (1 бал)	Методи та пристрої забезпечення захисту і безпеки (1 бал)	Захист, доступ та автентифікація (1 бал)	Основні напрями розвитку сучасної криптографії (1 бал)	Механізми та протоколи керування ключами (1 бал)	Шифрування даних (1 бал)
Лабораторні заняття (теми, бали)		Основи безпеки інформаційних ресурсів (11 балів)	Організаційний та правовий захист інформації (11 балів)	Основи інженерно-технічного захисту інформації (11 балів)	Механізми і політики розмежування прав доступ (11 балів)	Методи та пристрої забезпечення захисту і безпеки (11 балів)	Захист, доступ та автентифікація (22 бали)	Основні напрями розвитку сучасної криптографії (11 балів)	Механізми та протоколи керування ключами (11 балів)	Шифрування даних (11 балів)
Самостійна робота	Самостійна робота (5 балів)				Самостійна робота (5 балів)			Самостійна робота (10 балів)		
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)				Модульна контрольна робота 2 (20 балів)			Модульна контрольна робота 3 (20 балів)		
Підсумковий контроль (вид, бали)	Екзамен (40 балів)									

8. Рекомендовані джерела

Основна (базова):

1. Есин В. И., Кузнецов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.
2. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.
3. Домарев В. В. Безопасность информационных технологий: Системный подход: - К.: ООО "ТИД ДС", 2004. – 992с.
4. Конев И. Р., Беляев А. В. Информационная безопасность предприятия.- СПб.: БХВ - Петербург, 2003, 752с.: ил.

Додаткова

1. Белов Е. Б., Лось В. П., Мещеряков Р. В., Шелупанов А. А. Основы информационной безопасности. Учебное пособие для вузов - М.: Горячая линия - Телеком, 2006. - 544 с: ил.
2. Биячуев Т. А. / под ред. Л. Г.Осовецкого Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004.- 161 с.
3. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М.: Логос, 2001. - 264 с : ил.
4. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. 452с., ил.
5. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов.-М: Горячая линия-Телеком, 2004. -280 с.
6. Малюк А. А., Пазизин С. В., Погожин Н.С. Введение в защиту информации в автоматизированных Системах. - М.: Горячая линия-Телеком, 2001. - 148 с: ил.
7. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. – СПб.: Питер, 2002.- 848 с.: ил.
8. Мельников В. В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 1997.- 368с.:ил.
9. Шеннон К. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333-369 (Перевод В.Ф.Писаренко)
10. Козлов Д. А., Парандовский А. А., Парандовский А. К. Энциклопедия компьютерных вирусов. - М.: «СОЛОН-Р», 2001.
11. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина.-2-е изд., перераб. и доп.-М.: Радио и связь, 2001.- 376 с: ил.
12. Фергюсон Н., Шнайер Б. Практическая криптография. : Пер. с англ. — М.: Издательский дом "Вильямс", 2005. — 424 с. : ил.
13. Хорошков В. А., Чекатков А. А. Методы и средства защиты информации / Под ред. Ю. С. Ковтанюка – К.: Издательство Юниор, 2003.- 504с., ил.
14. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. - М.: "Триумф", 2002
15. Zachman John A., «Enterprise Architecture: The Past and the Future» Article published in DM Review Magazine. December 1999 Issue.
16. The Zachman Framework™: A Concise Definition, http://zachmaninternational.com.
17. Introducing The Open Group Architecture Framework (TOGAF), http://www.ibm.com.
18. Service-Oriented Architecture and Enterprise Architecture, http://www.ibm.com.
19. Microsoft Operations Framework; Cross Reference ITIL v3 and MOF 4.0. Microsoft Corporation. May 2009. http://go.microsoft.com/fwlink/?LinkId=151991.

9. Додаткові ресурси

1. http://ito.vspu.net/Prakt_IT/PIDSUMOK/2014-2015/rob/Klochenok/tzi.html

2. Автоматизована система "ВНЗ"