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
«_31_» ___01_____ 2019 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНФОРМАЦІЙНА БЕЗПЕКА ПРОГРАМНИХ СИСТЕМ»

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 № 2046/19
(підпис) (прізвище, ініціали)
«___» _____ 20 19 р.

Київ – 2019

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 16.01.2019 р. № 1

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	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	5 / 150	
Курс	4	
Семестр	8	
Кількість змістових модулів з розподілом:	5	
Обсяг кредитів	5	
Обсяг годин, в тому числі:	150	
Аудиторні	70	
Модульний контроль	10	
Семестровий контроль	-	
Самостійна робота	70	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Інформаційна безпека програмних систем» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 6.040302 Інформатика.

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

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Інформаційна безпека програмних систем» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Інформаційна безпека програмних систем» складається з п'яти змістових модулів: Захист програмного забезпечення шляхом блокування доступу до комп'ютера, Основні складові програми BIOS, Захист основних операційних систем, Захист програмного продукту, Інноваційні технології захисту інформації. Обсяг дисципліни – 150 год (5 кредитів).

Метою викладання навчальної дисципліни «Інформаційна безпека програмних систем» є вивчення принципів побудови та використання програмних та програмно-апаратних засобів для захисту програмного забезпечення та іншої інформації в комп'ютерних системах.

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 «Інформаційна безпека програмних систем» студенти повинні

знати:

– об'єкти програмного забезпечення, на які можливі атаки з боку комп'ютерних хакерів, та методи здійснення несанкціонованого доступу до інформації;

– принципи функціонування вбудованих засобів захисту комп'ютерних систем (BIOS) та шляхи протидії спробам їх взлому;

– принципи функціонування систем захисту, призначення привілей, зберігання паролів та автентифікація користувачів в операційних системах WINDOWS 9x, WINDOWS 2k (NT) та UNIX, методи хакерів з несанкціонованого проникнення до інформації, привласнення привілей адміністратора тощо;

– методи несанкціонованого зйому та навмисного пошкодження інформації та засоби протидії цим спробам;

– методи побудови захисту окремих програмних продуктів;

– основні прийоми і програмні засоби для аналізу та дизасемблювання програмних продуктів з метою їх подальшого несанкціонованого використання, методи захисту від дизасемблювання.

уміти:

– виконати аналіз безпеки комп'ютерної системи та усунути можливі шляхи

несанкціонованого доступу;

– здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації;

– виконувати адміністрування прав доступу до комп’ютерної системи з метою перешкоди призначення невиправданих привілей;

– виконувати постійний моніторинг з пошуку програмних закладок та каналів витоку інформації;

– використовувати основні прийоми та програмні засоби хакерів для перевірки надійності захисту інформації та стійкості його щодо хакерських атак. забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації;

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. Захист програмного забезпечення шляхом блокування доступу до комп'ютера							
Тема 1. Поняття інтелектуальної власності. Важливість захисту програмного забезпечення в сучасних умовах.	9	2			2		5
Тема 2. Причини існування комп'ютерних злодіїв. Методи проникнення до інформації у комп'ютері (хакінґ, крекінг, фрікінг). Класифікація методів та засобів захисту програмного забезпечення.	11	4			2		5
Тема 3. Апаратні, програмні та програмно-апаратні засоби захисту інформації. Носії ключової інформації (дискети, електронні ключі, SMART-карти, пристрої Touch-Memory). Прив'язка програмного забезпечення до унікальних характеристик комп'ютерної системи та BIOS.	11	2			4		5
Модульний контроль	2						
Разом	33	8			8		15
Змістовий модуль 2. Основні складові програми BIOS							
Тема 1. Принципи хешірования та зберігання паролів доступу. Інженерний пароль, старий та новий формат паролю, місце зберігання інженерного паролю в BIOS. Програмний пароль, місце знаходження програмних паролів (SUPERVISOR та USER) в CMOS-пам'яті	9	2			2		5
Тема 2. Засоби аналізу парольного хеша. Методи зняття, взлому та підбору паролю.	11	4			2		5

Програмні засоби хакерів для зняття та взлому паролю BIOS.							
Тема 3. Рекомендації щодо унеможливлення несанкціонованого доступу до комп'ютеру.	11	2			4		5
Модульний контроль	2						
Разом	33	8			8		15
Змістовий модуль 3. Захист основних операційних систем							
Тема 1. Побудова захисту ОС WINDOWS 2k (NT). Файлова система NTFS, її роль у захисті інформації. Принципи адміністрування у ОС WINDOWS 2k.	9	2			2		5
Тема 2. Особливості функціонування ОС *NIX. Система доступу та реєстрації користувачів у ОС UNIX та LINUX. Базові консольні команди *NIX та система каталогів	9	2			2		5
Тема 3 Класифікація засобів, що використовують при зломі програм. Методи аналізу програм із допомогою HEX-редакторів, дизасемблерів та відладчиків. Послідовність дій при зломі програмного продукту. Виготовлення CRACK-файлів	11	4			2		5
Модульний контроль	2						
Разом	31	8			6		15
Змістовий модуль 4. Захист програмного продукту							
Тема 1. Методика захисту програмних продуктів від несанкціонованого копіювання.	9	2			2		5
Тема 2. Технологія прив’язки програм до клієнтського апаратного та програмного забезпечення.	14	4					10
Тема 3 Особливості захисту текстової інформації. Приклади реалізації.	4	2			2		
Модульний контроль	2						
Разом	29	8			4		15
Змістовий модуль 5. Інноваційні технології захисту інформації							
Тема 1. Інноваційні технології захисту інформації	4	2			2		
Тема 2. Багаторівневе шифрування даних.	9	2			2		5
Тема 3 Сучасні інноваційні технології захисту інформації.	9	4					5
Модульний контроль	2						
Разом	24	8			4		10
Усього	150	40			30		70

5. Програма навчальної дисципліни

<u>Змістовий модуль 1</u>. Захист програмного забезпечення шляхом блокування доступу до комп'ютера

Основні питання:

- Поняття інтелектуальної власності. Важливість захисту програмного забезпечення в сучасних умовах
- Причини існування комп'ютерних злодіїв. Методи проникнення до інформації у комп'ютері (хакінг, крекінг, фрікінг). Класифікація методів та засобів захисту програмного забезпечення
- Апаратні, програмні та програмно-апаратні засоби захисту інформації. Носії ключової інформації (дискети, електронні ключі, SMART-карти, пристрої Touch-Memory). Прив'язка програмного забезпечення до унікальних характеристик комп'ютерної системи та BIOS.

Змістовий модуль 2. Основні складові програми BIOS

Основні питання:

- Принципи хешування та зберігання паролів доступу. Інженерний пароль, старий та новий формат паролю, місце зберігання інженерного паролю в BIOS. Програмний пароль, місце знаходження програмних паролів (SUPERVISOR та USER) в CMOS-пам'яті
- Засоби аналізу парольного хеша. Методи зняття, взлому та підбору паролю. Програмні засоби хакерів для зняття та взлому паролю BIOS.
- Рекомендації щодо унеможливлення несанкціонованого доступу до комп'ютеру

Змістовий модуль 3. Захист основних операційних систем

Основні питання:

- Побудова захисту ОС WINDOWS 2k (NT). Файлова система NTFS, її роль у захисті інформації. Принципи адміністрування у ОС WINDOWS 2k.
- Особливості функціонування ОС *NIX. Система доступу та реєстрації користувачів у ОС UNIX та LINUX. Базові консольні команди *NIX та система каталогів
- Класифікація засобів, що використовують при зломі програм. Методи аналізу програм із допомогою HEX-редакторів, дизасемблерів та відладчиків. Послідовність дій при зломі програмного продукту. Виготовлення CRACK-файлів

Змістовий модуль 4. Захист програмного продукту

Основні питання:

- Методика захисту програмних продуктів від несанкціонованого копіювання.
- Технологія прив’язки програм до клієнтського апаратного та програмного забезпечення
- Особливості захисту текстової інформації. Приклади реалізації.

Змістовий модуль 5. Інноваційні технології захисту інформації

Основні питання:

- Інноваційні технології захисту інформації
- Багаторівневе шифрування даних.
- Сучасні інноваційні технології захисту інформації..

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної 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	Модуль 4	Модуль 5

	максимальна кількість балів за одиницю	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	4	4	4	4	4	4	4	4	4	4
Відвідування семінарських занять	1										
Відвідування практичних занять	1										
Відвідування лабораторних занять	1	4	4	4	4	3	3	2	2	2	2
Робота на семінарському занятті	10										
Робота на практичному занятті	10										
Лабораторна робота (в тому числі допуск, виконання, захист)	10	4	40	4	40	3	30	2	20	2	20
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25	1	25	1	25
Виконання ІНДЗ	30										
Разом		-	78	-	78	-	67	-	56	-	56
Максимальна кількість балів: 335											
Розрахунок коефіцієнта: 335/100=3,35											

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. Захист програмного забезпечення шляхом	15	5

	блокування доступу до комп'ютера		
1	Основні методи блокування доступу до інформації в програмному забезпеченні • виконання завдань відповідно до теми; • опрацювання фахових видань.	15	5
Змістовий модуль 2. Основні складові програми BIOS		15	5
2	Аналіз методів і засобів несанкціонованого здобуття інформації програми BIOS • виконання завдань відповідно до теми; • опрацювання фахових видань.	15	5
Змістовий модуль 3. Захист основних операційних систем		15	5
3	Методи захисту операційної системи Unix: • виконання завдань відповідно до теми; • опрацювання фахових видань.	15	5
Змістовий модуль 4. Захист програмного продукту		15	5
4	Закон України про авторське право на програмне забезпечення: • виконання завдань відповідно до теми; • опрацювання фахових видань.	15	5
Змістовий модуль 5. Інноваційні технології захисту інформації		10	5
5	Біометричні системи захисту інформації: • виконання завдань відповідно до теми; • опрацювання фахових видань.	10	5
	Разом	70	25

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 заліку, умовою допуску до якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

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: 150 год., лекції – 40 год., лабораторні роботи – 30 год., модульний контроль – 10 год., самостійна робота –70 год.

Модулі (назви, бали)	**Змістовий модуль 1. Захист програмного забезпечення шляхом блокування доступу до комп'ютера (78 балів)**			**Змістовий модуль 2. Основні складові програми BIOS (78 балів)**			**Змістовий модуль 3. Захист основних операційних систем (67 балів)**			**Змістовий модуль 4. Захист програмного продукту (56 балів)**			**Змістовий модуль 5. Інноваційні технології захисту інформації (56 балів)**		
Лекції (теми, бали)	Поняття інтелектуальної власності. Важливість захисту програмного забезпечення в сучасних умовах. (1 бал)	Причини існування комп'ютерних злодіїв. Методи проникнення до інформації у комп'ютері (хакінґ, крекінг, фрікінг). (1 бал)	Апаратні, програмні та програмно-апаратні засоби захисту інформації. Носії ключової інформації (2 бали)	Принципи хешірования та зберігання паролів доступу. Інженерний пароль, старий та новий формат паролю, місце зберігання інженерного паролю в BIOS. (1 бал)	Засоби аналізу парольного хеша. Методи зняття, взлому та підбору паролю. Програмні засоби хакерів для зняття та взлому паролю BIOS. (1 бал)	Рекомендації щодо унеможливлення несанкціонованого доступу до комп'ютеру. (2 бали)	Основні напрями розвитку сучасної криптографії (1 бал)	Механізми та протоколи керування ключами (1 бал)	Класифікація засобів, що використовують при зломі програм. (2 бали)	Методика захисту програмних продуктів від несанкціонованого копіювання. (1 бал)	Технологія прив’язки програм до клієнтського апаратного та програмного забезпечення. (2 бали)	Особливості захисту текстової інформації. Приклади реалізації (1 бал))	Інноваційні технології захисту інформації (1 бал)	Багаторівневе шифрування даних. (1 бал)	Сучасні інноваційні технології захисту інформації. (2 бали)

Лабораторні заняття (теми, бали)	Дослідження системи захисту комп'ютера з допомогою BIOS (11 балів)	Огляд складових інформаційної безпеки (11 балів)	Огляд методів та засобів захисту інформації (22 бали)	Структура PE-файлів (11 балів)	Дослідження захисту операційної системи WINDOWS 2k. (11 балів)	Адміністрування безпеки операційної системи WINDOWS 2k (22 бали)	Дослідження атак з допомогою штучно занесених програм класу SpyWare. (11 балів)	Мережеві сканери та екрани (11 балів)	Шифрування даних (11 балів)	Дослідження захисту операційної системи WINDOWS 2k. (11 балів)	Адміністрування безпеки операційної системи WINDOWS 2k (11 бали)		Структура PE-файлів (11 балів)	Мережеві сканери та екрани (11 балів)		
Самостійна робота	Самостійна робота (5 балів)			Самостійна робота (5 балів)			Самостійна робота (5 балів)			Самостійна робота (5 балів)			Самостійна робота (5 балів)			
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)			Модульна контрольна робота 2 (25 балів)			Модульна контрольна робота 3 (25 балів)			Модульна контрольна робота 4 (25 балів)			Модульна контрольна робота 5 (25 балів)		
Підсумковий контроль (вид, бали)	Залік															

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"