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 «ТЕХНОЛОГІЇ БЕЗПЕКИ БЕЗПРОВОДОВИХ І МОБІЛЬНИХ МЕРЕЖ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	другого (магістерського)
освітньої програми	125.00.02 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 0962/18
(підпис) (прізвище, ініціали)
«___» _____ 20 18 р.

Київ – 2018

Розробники:

Соколов Володимир Юрійович, старший викладач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Викладачі:

Соколов Володимир Юрійович, старший викладач 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 125.00.02 Безпека інформаційних і комунікаційних систем)

___.___. 20___ р.

Керівник освітньої програми _____ (В.Л. Бурячок)
(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	7 / 210	
Курс	5	
Семестр	9	
Кількість змістових модулів з розподілом:	3	
Обсяг кредитів	7	
Обсяг годин, в тому числі:	210	
Аудиторні	56	
Модульний контроль	12	
Семестровий контроль	60	
Самостійна робота	82	
Форма семестрового контролю	Екзамен, курсова робота	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Технології безпеки мережевої інфраструктури» 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 навчальних планів спеціальності 125 «Кібербезпека».

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 «Технології безпеки мережевої інфраструктури» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Технології безпеки мережевої інфраструктури» складається з 3-х змістових модулів: 1. Сутність вразливостей мережевої інфраструктури. Класифікація загроз. Аналіз дій хакерів і інсайдерів. 2. Попередження експлуатації вразливостей мережевої інфраструктури. 3. Методи захисту периметрів об'єктів мережевої інфраструктури. Обсяг дисципліни – 210 год (7 кредитів).

Метою викладання навчальної дисципліни «Технології безпеки мережевої інфраструктури» є отримання компетентностей в області захисту об'єктів мережевої інфраструктури від несанкціонованого доступу до ресурсів.

Завдання:

- надання студентам теоретичних знань щодо проблем, завдань і особливостей технологій безпеки мережевої інфраструктури;
- формування у студентів категоріальних понять з основ процесів, що притаманні функціонуванню технологій безпеки мережевої інфраструктури в умовах зовнішніх і внутрішніх негативних впливів;
- формування у студентів знань і умінь щодо проведення аудиту безпеки об'єктів і інформаційно-комунікаційних систем мережевої інфраструктури;

– стимулювання студентів до активної аналітико-пошукової роботи, що спрямована на визначення ефективних шляхів розвитку у сфері захисту інформації.

– **У результаті вивчення навчальної дисципліни формуються**

загальні компетентності:

КЗ-2: Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях

КЗ-3: Здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням.

фахові компетентності:

КФ-1: Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації

КФ-5: Здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації.

3. Результати навчання за дисципліною

При вивченні курсу «Технології безпеки мережевої інфраструктури» студенти повинні

знати:

- про джерела і способи дії загроз на об’єкти і інформаційно-комунікаційні системи мережевої інфраструктури;
- про правові і нормативні акти, які визначають систему захисту інформації в державі;
- про основні методи, технології, принципи і правила побудови захисту об’єктів і інформаційно-комунікаційних систем мережевої інфраструктури;
- про алгоритми створення сучасних технологій забезпечення безпеки мережевої інфраструктури;
- про методи та технології проведення аудиту безпеки технологій мережевої інфраструктури.

уміти:

- використовувати технології забезпечення безпеки мережевої інфраструктури;
- визначати технології, принципи і правила побудови захисту об’єктів і інформаційно-комунікаційних систем мережевої інфраструктури;
- створювати засобами стандартного програмного забезпечення елементи захисту інформації.

та досягнути наступні ***програмні результати***:

ПРз-2	- вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки; - вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні та/або безпекові технології у сфері захисту інформації; - знати уразливості й методи їх застосування в різних телекомунікаційних технологіях; - знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж; - вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи; - знати методи організації захищеної передачі даних у незахищеному середовищі;
ПРз-3	- знати уразливості й методи їх застосування в безпроводових і мобільних мережах; - вміти виявляти загрози проникнення або доступу зловмисників до таких мереж; - знати спеціалізоване мережеве обладнання, що застосовується для забезпечення

	безпеки безпроводових і мобільних мереж; - вміти проектувати захищені (з урахуванням загроз) безпроводові мережі;
ПРз-7	- знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки; - вміти знаходити шляхи для їх усунення;
ПРз-9	- володіти практичними навичками проведення аудиту безпеки ІКС, їх адміністрування та експлуатації; - вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічног

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. Сутність вразливостей мережевої інфраструктури. Класифікація загроз. Аналіз дій хакерів і інсайдерів							
Тема 1.Концепція забезпечення безпеки ІТ-інфраструктури і засоби її реалізації	24	4		4	2		14
Тема 2.Типові корпоративні мережі, вразливості і атаки.	24	4		2	4		14
Модульний контроль	4						
Разом	52	8		6	6		28
Змістовий модуль 2. Попередження експлуатації вразливостей мережевої інфраструктури							
Тема 3**.** Хакерські атаки, засоби, утиліти.	10	2		2			6
Тема 4. Мережеві хробаки.	10	2		2			6
Тема 5**.** Хакерські утиліти.	10	2		2			6
Тема 6. Технології захисту мережевої інфраструктури.	16	2			6		8
Модульний контроль	4						
Разом	50	8		6	6		26
Змістовий модуль 3. Методи захисту периметрів об’єктів мережевої інфраструктури							
Тема 7. Аудит безпеки мережевої інфраструктури.	22	2		4	2		14
Тема 8. Захист периметрів об’єктів мережевої інфраструктури.	22	2		2	4		14
Модульний контроль	4						
Разом	48	4		6	6		28
Курсова робота	30						
Підготовка та проходження контрольних заходів	30						
Усього	210	20		18	18		82

5. Програма навчальної дисципліни

Змістовий модуль 1. Сутність вразливостей мережевої інфраструктури. Класифікація загроз. Аналіз дій хакерів і інсайдерів

Тема 1. Вступ. Концепція забезпечення безпеки ІТ-інфраструктури і засоби її реалізації

Інормаційна і кібернетична безпека. Политика безпеки мережевої інфраструктури. Автентифікаія. Суб'єкти і об'єкти. Поняття аудиту. Події порушення політики безпеки. Засоби криптографічного захисту інформації. Захист периметру інформаційно-комунікаційних систем. Служби і протоколи віддаленого доступу.

Тема 2. Типові корпоративні мережі, вразливості і атаки

Рівні інформаційної інфраструктури. Загрози інформації. Вразливості об'єктів і систем інформаційної інфраструктури. Атаки на складові інформаційної інфраструктури. Класифікація атак за мотивованістю.

Змістовий модуль 2. Попередження експлуатації вразливостей мережевої інфраструктури

Тема 3. Хакерські атаки, засоби, утіліти

Цілі і засоби проведення хакерських атак. Застосування технологій комп'ютерних вірусів, троянських коней, поштових хробаків, сніферів, Rootkit, прпеціального програмного забезпечення. Засоби ведення мережевої розвідки. Застосування технологій соціальної інженерії.

Тема 4. Мережеві хробаки

Типи мережевих хробаків і технології експлуатації вразливостей мережевої інфраструктури. Технології захисту від хакерських утиліт.

Тема 5. Хакерські утіліти

Мережеві атаки. Утиліти несанкціонованого проникнення в мережеві інфраструктури. Конструктори вірусів і троянських програм. Поліморфні генератори..

Тема 6. Технології захисту мережевої інфраструктури

Технології антивірусних програмних засобів. Евристичний аналіз. Міжмережеві екрани. Проактивні технології безпеки мережевої інфраструктури.

Змістовий модуль 3. Методи захисту периметрів об'єктів мережевої інфраструктури

Тема 7. Аудит безпеки мережевої інфраструктури

Нормативні документи і державні стандарти безпеки інформаційно-комунікаційних систем. Цілі, методи і засоби проведення аудиту стану безпеки мережевої інфраструктури. Документальне оформлення результатів аудиту. Модель загроз, Модель порушника, Політика інформаційної безпеки мережевої інфраструктури.

Тема 8. Захист периметрів об'єктів мережевої інфраструктури

Топологія побудови мережевої інфраструктури. Модель OSI. Стек мережевих протоколів. Демілітаризована зона мережевої інфраструктури. Технології забезпечення безпеки периметрів мережевих інфраструктур і інформаційно-комунікаційних систем.

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	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	4	4	4	4	2	2
Відвідування семінарських занять							
Відвідування практичних занять	1	3	3	3	3	3	3
Відвідування лабораторних занять	1	3	3	3	3	3	3
Робота на семінарському занятті							
Робота на практичному занятті	10	3	30	3	30	3	30
Лабораторна робота (в тому числі допуск, виконання, захист)	10	3	30	3	30	3	30
Виконання завдань для самостійної роботи	5	2	10	2	10	2	10
Виконання модульної роботи	25	1	25	1	25	1	25
Разом		-	105	-	105	-	103
Максимальна кількість балів: 313							
Розрахунок коефіцієнта: 313/60=5,22							

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. Сутність вразливостей мережевої інфраструктури. Класифікація загроз. Аналіз дій хакерів і інсайдерів.		28	10
1	Тема 1. Концепція забезпечення безпеки ІТ-інфраструктури і засоби її реалізації. Тема 2. Типові корпоративні мережі, вразливості і атаки.	28	10
Змістовий модуль 2. Асиметричні криптосистеми на базі кілець		26	10
2	Тема 3. Хакерські атаки, засоби, утиліти. Тема 4. Мережеві хробаки. Тема 5. Хакерські утиліти. Тема 6. Технології захисту мережевої інфраструктури.	26	10
Змістовий модуль 3. Асиметричні криптосистеми на базі полів		28	10

3	Тема 7. Аудит безпеки мережевої інфраструктури. Тема 8. Захист периметрів об’єктів мережевої інфраструктури.	28	10
	Разом	82	30

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.	4 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв’язання проблеми, визначення перспектив дослідження	4 бали
3	Дотримання вимог щодо технічного оформлення	2 бали
	Разом	10 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.

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 семестрового контролю

1. Загрози безпеки комп’ютерних мереж і систем.
2. Політика безпеки.
3. Ідентифікація і автентифікація.

4. Протоколи і технології доступу до ресурсів інформаційно-комунікаційних систем.
5. Поняття архітектури відкритих ключів.
6. Принципи захисту периметру інформаційної інфраструктури.
7. Призначення і основні інженерні рішення технології Radius.
8. Віртуальні мережі. Принципи і протоколи.
9. Рівні інформаційної інфраструктури корпоративної інформаційно-комунікаційної системи.
10. Загальні принципи атаки на інформаційну інфраструктуру.
11. Поняття загроз, вразливостей і атак на інформаційні інфраструктури.
12. Класифікація вразливостей об'єктів, протоколів і служб IP-мереж за рівнем в інформаційній інфраструктурі.
13. Класифікація вразливостей інформаційної інфраструктури за причинами виникнення.
14. Класифікація вразливостей інформаційної інфраструктури за рівнем (ступенем) ризику.
15. Класифікація атак в IP-мережах.
16. Вразливості технологій електронної пошти.
17. Експлуатація вразливостей Веб-додатків.
18. Експлуатація вразливостей слабких паролів при управлінні доступом..
19. Хакерські технології ведення інформаційної розвідки.
20. Інформаційна розвідка, Сніфінг пакетів даних.
21. Експлуатація вразливостей інформаційної інфраструктури при здійсненні IP-спуфінгу.
22. Експлуатація вразливостей інформаційної інфраструктури при здійсненні атаки Man-in-the-Middle.
23. Способи здійснення атаки «Ін'єкція» в мережевій інфраструктурі.
24. Використання можливостей соціальної інженерії при впливі на функціонування мережевої інфраструктури.
25. Основні способи проникнення комп'ютерних хробаків в мережеву інфраструктуру.
26. Хакерські утиліти, характеристики і технологічна реалізація при експлуатації вразливостей мережевої інфраструктури.
27. Антивірусні програмні засоби. Принципи функціонування.
28. Принцип функціонування проактивних систем антивірусного захисту.
29. Технології евристичного аналізу при виявленні злоякісного програмного забезпечення в мережних інфраструктурах.
30. Виявлення ознак наявності злоякісного програмного забезпечення системними засобами мережних інфраструктур.
31. Основні завдання і напрямки робіт при проведенні аудиту безпеки мережевої інфраструктури.
32. Види аудиту інформаційної і кібернетичної безпеки.
33. Експертний аудит безпеки мережевої інфраструктури.
34. Програмні засоби проведення аудиту безпеки мережевої інфраструктури.
35. Документування результатів проведення аудиту мережевої інфраструктури.
36. Захист периметрів об'єктів мережевої інфраструктури.

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 карта дисципліни

Разом:210 год., лекції – 20 год., практичні заняття – 18 год., лабораторні роботи – 18 год., модульний контроль – 12 год., самостійна робота – 120 год., семестровий контроль – 30 год.

Модулі (назви, бали)	**Змістовий модуль 1** (105 балів)					**Змістовий модуль 2** (105 балів)					**Змістовий модуль 3** (103 бали)				
Лекції (теми, бали)	1. Тема 1 (1 бал)	2. Тема 1 (1 бал)	3. Тема 2 (1 бал)	4. Тема 2 (1 бал)		5.Тема 3 (1 бал)	6. Тема 4 (1 бал)	7. Тема 5 (1 бал)	8. Тема 6 (1 бал)		9. Тема 7 (1 бал)	10. Тема 8 (1 бал)			
Лабораторні заняття (теми, бали)			1. (11 балів)	2. (11 балів)	3. (11 балів)			4. (11 балів)	5. (11 балів)	6. (11 балів)			7. (11 балів)	8. (11 балів)	9. (11 балів)
Практичніі заняття (теми, бали)			1. (11 балів)	2. (11 балів)	3. (11 балів)			4. (11 балів)	5. (11 балів)	6. (11 балів)			7. (11 балів)	8. (11 балів)	9. (11 балів)
Самост. робота	Самостійна робота (10 балів)					Самостійна робота (10 балів)					Самостійна робота (10 балів)				
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (20 балів)					Модульна контрольна робота 2 (20 балів)					Модульна контрольна робота 3 (20 балів)				
Підсумк. контроль	Екзамен (40 балів)														

8. Рекомендовані джерела

Основна

1. Скабцов Н. Аудит безопасности информационных систем. - СПб.: Питер, 2018.– 272с.
2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и Техника, 2004. – 384с.
3. Безруков Н.Н. Компьютерная вирусология: справочное руководство. – Киев: УРЕ, 1991. – 416с.
4. Домарев В.В. Защита информации и безопасность компьютерных систем. - К.: Издательство «Диасофт», 1999. – 480с.
5. Курило А.П. Аудит информационной безопасности / А.П.Курило, С.Л.Зефиров, В.Б.Голованов - М.: Издательская группа «БДЦ-пресс", 2006 — 304с.
6. Таненбаум Э. Компьютерные сети. 4-е изд. . - СПб.: Питер, 2003.– 992с.
7. Максимов Н.В. Архитектура ЭВМ и вычислительных систем: Учебник / Н.В.Максимов, Т.Л.Партыка, И.И.Попов - М.: ФОРУМ ИНФРА-М, 2005. — 512с. с.
8. Прата Стивен Язык программирования С++. Лекции и упражнения. Учебник: Пер. с англ. - СПб.: ООО «ДиаСофтЮП», 2005. – 1104с.Питер, 2018.– 272с.
9. Стрелковська І.В. Дискретна математика: навч.посіб. /І.В.Стрелкоська, А.Г.Буслаєв, О.М.Харсун, Т.Л.Пашкова, М.І.Баранов, Т.І.Григор'єва, В.М.Вишневська, Л.Л.Кольцова. – Одеса: ОНАЗ ім.. О.С.Попова, 2010. – 196с.

9. Інформаційні ресурси

1. Web сайт: www.Wikipedia.com
2. Продуктb Google [Електронний ресурс] // – Режим дост.: http://www.google.com.ua/intl/ru/ about/products/ – Заголовок з екрана