Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ О.О. Ілляшенко
(підпис) (ініціали та прізвище)

«31» серпня 2021 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Комплексні системи захисту інформації: проектування, впровадження, супровід
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

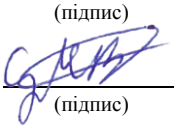
Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

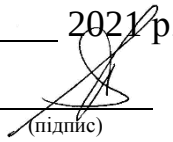
Харків 2021 рік

Розробник: Пєвнєв В.Я., доцент кафедри 503, к.т.н., доцент 
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Цуранов М.В., ст. викладач кафедри 503 
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 30 » 08 2021 р.

Завідувач кафедри д.т.н., професор  В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4</td><td rowspan="11">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека"
(код та найменування)

Освітня програма
Безпека інформаційних і комунікаційних систем
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 2</td><td>2021/2022</td></tr>
<tr><td>Індивідуальне завдання: РГР</td><td rowspan="2">Семестр: 7-й</td></tr>
<tr><td>Загальна кількість годин – 64/120</td></tr>
<tr><td rowspan="7">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи студента – 3,5</td><td>Лекції *</td></tr>
<tr><td>32 годин</td></tr>
<tr><td>Практичні, семінарські *</td></tr>
<tr><td>32 годин</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>56 годин</td></tr>
<tr><td>Індивідуальні завдання:</td></tr>
<tr><td>6 годин</td></tr>
<tr><td>Вид контролю:</td></tr>
<tr><td>модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:
Для денної форми навчання – 64/56.

*Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: діяльності на основі застосування системи теоретичних знань і практичних навичок з виявлення способів порушення інформаційної безпеки при роботі комп'ютерних систем обробки інформації; вирішення задач захисту програм та даних програмно-апаратними засобами; застосування системного підходу до забезпечення інформаційної безпеки, включаючи комплекс організаційних заходів.

Завдання: застосовувати знання до вирішення задач інформаційної безпеки; обирати потрібні організаційні та інженерно-технічні заходи, засоби і методи захисту інформації; аналізувати вхідні данні та обирати методи оцінки якості.

Компетентності, які набуваються:

- здатність застосовувати знання у практичних ситуаціях.
- знання та розуміння предметної області та розуміння професії.
- здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
- вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
- здатність до пошуку, оброблення та аналізу інформації.
- здатність забезпечувати неперервність бізнесу згідно встановленої політики 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 відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.
- здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
- здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
- здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки.
- здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
- здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
- здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Очікувані результати навчання:

- застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
- організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
- використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
- аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
- адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
- готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
- впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
- виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
- виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;
- розробляти моделі загроз та порушника;
- аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
- вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
- використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
- реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
- забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
- використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

- застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
- вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
- аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;
- здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
- здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
- застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
- вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
- вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
- приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
- вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
- вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;

- виявляти небезпечні сигнали технічних засобів;
- вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;
- інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
- проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
- інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
- забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
- впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
- застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;
- вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;
- застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
- здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
- вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
- забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
- забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

Пререквізити – дисципліна є обов'язковим компонентом освітній програми і базується на знаннях, отриманих під час вивчення «Захист інформації в інформаційно-комунікаційних системах», «Прикладна криптологія», «Надійність та

функціональна безпека інформаційно-управляючих систем», «Системи технічного захисту інформації».

Кореквізити – «Комплексні системи захисту інформації: проектування, впровадження, супровід», «Комплексні системи захисту інформації: проектування, впровадження, супровід (КП)», «Дипломний робота (проект) бакалавра».

3. Програма навчальної дисципліни

Модуль 1

Змістовний модуль 1. Основи теорії захисту інформації.

ТЕМА 1. Вступна

Визначення комплексної системи захисту інформації. Етапи побудови КСЗІ. Принципи побудови КСЗІ.

ТЕМА 2. Архітектура безпеки ІТС

Загрози безпеки для ІТС. Застосування сервісів безпеки до рівнів безпеки ІТС.

ТЕМА 3. Міжнародні стандарти архітектури безпеки ІТС

ITU-T Rec. X.805. Security architecture for systems providing end-to-end communications. ITU-T Rec. X.800 (1991). Security architecture for Open Systems Interconnection for CCITT applications. ITU-T E.408. Telecommunication networks security requirements.

ТЕМА 4. Моделі захисту інформації

Визначення суб'єктів та об'єктів в моделях ЗІ. Мандатні моделі ЗІ. суб'єктно-об'єктні моделі ЗІ.

ТЕМА 5. Монітори безпеки

МБО. МБС. ІПС. Ядро безпеки.

ТЕМА 6. Визначення інформації яка потребує захисту.

Методика визначення інформації яка потребує захисту. Класифікація інформації. Проблеми визначення інформації.

ТЕМА 7. Визначення вартості інформації

Проблема визначення вартості інформації. Економічні методики визначення вартості інформації. Методика Дж. Кантера.

ТЕМА 8. Особливості об'єктів захисту

Категорії об'єктів захисту. Особливості охорони різних типів об'єктів. Структура системи забезпечення безпеки об'єктів.

Модульний контроль.

Модуль 2

Змістовний модуль 2. Канали витоку інформації. Засоби контролю.

ТЕМА 9. Побудова комплексної системи охорони периметру

Загальні принципи забезпечення безпеки об'єктів. Системи охоронно-тривожної сигналізації. Охоронні сповіщувачі. АРМ охоронної системи.

ТЕМА 10. Система контролю та управління доступом

Класифікація СКУД. Призначення СКУД. Електронна прохідна. Датчики СКУД.

ТЕМА 11. Системи телевізійного спостереження

Визначення та призначення. Класифікація. Відеокамери. АРМ системи відео нагляду.

ТЕМА 12. Системи пожежної сигналізації

Визначення та призначення. Класифікація. Сповіщувачі. Оповіщувачи. Система автоматичного пожежогасіння.

ТЕМА 13. Охорона периметру

Визначення та призначення. Зони охорони. Оптимізація побудови охорони периметру. Системи охорони периметру.

ТЕМА 14. Методи контролю доступу в КСЗІ

Захист доступу до ОТ за допомогою електронних брелоків та смарт-карт. Засоби біометричного захисту доступу до ОТ.

ТЕМА 15. Технічний контроль ефективності засобів захисту інформації

Види контролю. Способи проведення. Методи технічного контролю.

ТЕМА 16. Акустичний та вібро акустичний контроль

Методика контролю. Склад системи контролю. Контроль речового діапазону. Засоби контролю.

Модульний контроль.

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1. Основи теорії захисту інформації.					
Тема 1. Вступна	5	2	2		1
Тема 2. Архітектура безпеки ІТС.	6	2	2		2
Тема 3. Міжнародні стандарти архітектури безпеки ІТС.	6	2	2		2
Тема 4. Моделі захисту інформації.	6	2	2		2
Тема 5. Монітори безпеки.	8	2	2		4
Тема 6. Визначення інформації яка потребує захисту.	8	2	2		4
Тема 7. Визначення вартості інформації.	9	2	2		5
Тема 8. Особливості об’єктів захисту.	9	2	2		5
Разом за змістовним модулем 1	57	16	16		25
Усього годин за модуль 1	57	16	16		25

Модуль 2					
Змістовний модуль 2. Канали витоку інформації. Засоби контролю.					
Тема 9. Побудова комплексної системи охорони периметру.	5	2	2		1
Тема 10. Система контролю та управління доступом.	6	2	2		2
Тема 11. Системи телевізійного спостереження.	6	2	2		2
Тема 12. Системи пожежної сигналізації.	6	2	2		2
Тема 13. Охорона периметру.	8	2	2		4
Тема 14. Методи контролю доступу в КСЗІ.	8	2	2		4
Тема 15. Технічний контроль ефективності засобів захисту інформації.	9	2	2		5
Тема 16. Акустичний та вібро-акустичний контроль.	9	2	2		5
РГР	6				6
Разом за змістовним модулем 2	63	16	16		31
Усього годин за модуль 2	63	16	16		31
Усього годин за дисципліною	120	32	32		56

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
...	*Не передбачено*	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Отримання практичних навичок з використання суб'єктно-об'єктних моделей доступу	4
2	Отримання практичних навичок з використання флеш карток в якості аутентифікатора.	4
3	Отримання практичних навичок з моніторингу ресурсів ПК.	4
4	Отримання практичних навичок з визначення вартості інформації.	4
5	Отримання практичних навичок з визначення радіусу контрольованої зони.	4
6	Отримання практичних навичок з підбору засобів периметрової охорони.	6
7	Отримання практичних навичок з виміру ПЕМВІН.	6
	Разом	**32**

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	2	3
	Не передбачено	

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Теорія захисту інформації. Моделі захисту інформації	10
2	Архітектура безпеки інформаційно-телекомунікаційних систем	10
3	Параметричні канали витоку інформації	10
4	Система пожежної охорони як частина КСЗІ	5
5	СКУД. Принципи побудови та використання.	5
6	Вивчення можливостей програмного засобу моделювання загроз MS Threat Modeling tool	10
7	РГР	6
	Разом	**56**

9. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
1	Побудова моделі загроз для аудиторій кафедри.	6

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
модуль 1			
Лекції	0…1	8	0…8
Практичні роботи	0...2	8	0…16
Модульний контроль	0…25	1	0..25
модуль 2			
Лекції	0…1	8	0…8
Практичні роботи	0…1	8	0…8
Модульний контроль	0…25	1	0…25
РГР	0…10	1	0…10
Усього за семестр			**0…100**

Контроль знань при проведенні занять оцінюється за такими шкалами:

активність на лекції під час відповідей на питання:

- повна відповідь на питання - 1 бал;
- неповна відповідь – 0,5 балу;
- відсутність на лекції - 0 балів,

виконання і захист практичних робіт:

при виконанні всіх вимог завдань методик на роботи - 2 бали;

- неповні відповіді на питання при захисті результатів роботи за змістом досліджуваної теми – 1,5 бали;
- неповні відповіді на питання за змістом і результатами роботи - 1 бал;
- недооформлені результати роботи і неповні відповіді на питання за змістом результатів роботи -0,5 балу;
- якщо робота не виконана і не захищена - 0 балів.

На модульний контроль (всього 25 балів) виносяться всі пройдені за контрольований період теми, які включаються в варіанти завдань, що містять по 25 питання (по всім темам та видам занять). Максимальна кількість балів за кожне питання - 1.

Семестровий контроль у вигляді іспиту проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних та одного практичного запитань, максимальна кількість за кожне із запитань, складає 33 балу.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 80% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняних та міжнародних стандартів для проведення наукових робіт та робіт щодо захисту інтелектуальної власності.

Добре (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 90% завдань практичних занять. Уміти використовувати сучасні методи теоретичних та експериментальних досліджень для організації та проведення наукових робіт.

Мати необхідний обсяг вмінь для одержання позитивної оцінки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Уміти виконувати інформаційне забезпечення наукових досліджень.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

1. Презентації лекцій.
2. Керівництво до практичних робіт.

14. Рекомендована література

Базова

1. Цуранов М.В. Методи та засоби боротьби з правопорушеннями в інформаційній сфері: навчальний посібник / М.В. Цуранов, В.М. Струков, В.Я. Пєвнєв. – Харків: ХНУВС, 2015. 256 с.
2. Домарєв В. В., Швець В. А., Шестакова В. В. Організаційне забезпечення захисту інформації з обмеженим доступом: Навчальний посібник. / Національний авіаційний університет; МОН. – К.: НАУ, 2006. 108 с.
3. Основы информационной безопасности : курс лекций : учебное пособие / Из-дание третье / Галатенко В.А. Под ред. Академика РАН В.Б. Бетелина / - М.:ИН-ТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. 208 с.
4. Архитектура компьютерных систем и сетей: Учеб. пособие / Т.П. Барановская, В.И. Лойко и др.; под ред. В.И. Лойко. – М.: Финансы и статистика, 2003. 256 с.: ил.

Допоміжна

1. Защита компьютерной информации от несанкционированного доступа. А. Ю. Щеглов. – СПб.: Издательство «Наука и Техника», 2004. 384 с.: ил.
2. Сердюк В.А. Организация и технология защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В. А. Сердюк ; Государственный университет - Высшая школа экономики .— Москва : ГУ ВШЭ, 2011 . 573 с.

15. Інформаційні ресурси

1. Архитектура комп’ютера [Электрон. ресурс]. - Режим доступа:

http://inf1.info/book/export/html/44

2. Вікіпедія — вільна енциклопедія [Электрон. ресурс]. - Режим доступа: http://www. ru.wikipedia.org/

3. Википедия — свободная энциклопедия [Электрон. ресурс]. - Режим доступа: http://www. ru.wikipedia.org/

4. Microsoft Virtual Academy [Электрон. ресурс]. - Режим доступа: http://www.microsoftvirtualacademy.com/

5. Microsoft IT Academy Program [Электрон. ресурс]. - Режим доступа: https://itacademy.microsoftelearning.com/

6. Cisco Networking Academy [Электрон. ресурс]. - Режим доступа: https://www.netacad.com/, http://www.cisco.com/web/learning/netacad/