Форма № 09/18
Затверджена рішенням вченої
ради ІДГУ
від 30.08.2018 р., протокол № 1

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ІЗМАЇЛЬСЬКИЙ ДЕРЖАВНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ УПРАВЛІННЯ, АДМІНІСТРУВАННЯ ТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ
КАФЕДРА МАТЕМАТИКИ, ІНФОРМАТИКИ ТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

«ЗАТВЕРДЖЕНО»
Навчально-методичною радою ІДГУ
Протокол № 4 від 15.01 2019 р.

Голова НМР _____ Н. М. Кольцун

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ
(назва навчальної дисципліни)

освітній ступінь бакалавр
(назва освітнього ступеня)

галузь знань 02 Культура та мистецтво, 01 Освіта
(шифр і назва галузі знань)

спеціалізація 029 Інформаційна, бібліотечна та архівна справа,
014.10 Трудове навчання та технології
(код і назва спеціальності)

освітня програма / Документознавство та інформаційна діяльність,
Середня освіта: Трудове навчання та технології, інформатика.
(код і назва спеціальності)

тип дисципліни вибіркова
(обов'язкова / вибіркова / факультативна)

Ізмаїл – 2018

ПОГОДЖЕНО:
Гарант освітньо-професійної програми
Кожухар Ж.В.
(підпис, ініціали, прізвище)

РЕКОМЕНДОВАНО:
кафедрою математики, інформатики та інформаційної діяльності
протокол № 11 від 27.06.18.

Завідувач кафедри Івлієва О.М
(підпис, ініціали, прізвище)

ПОГОДЖЕНО:
Голова науково-методичної ради факультету
ФУПД
Федорова О.В.
(підпис, ініціали, прізвище)

Розробники програми: викладачі кафедри математики, інформатики та інформаційної діяльності Дмитрієва М.В.

Рецензенти програми: викладачі кафедри математики, інформатики та інформаційної діяльності Дущенко О.С.

© автор(и), 2018
© ІДГУ, 2018

1. ОПИС ДИСЦИПЛІНИ

Найменування показників	**Розподіл годин за навчальним планом**	
	Денна	***Заочна***
Кількість кредитів: 4	*Лекції*:	
	22	*4*
Модулів:1	*Практичні заняття*:	
Загальна кількість годин:120	-	-
Рік вивчення дисципліни за навчальним планом: 2	*Лабораторні заняття:*	
	26	*8*
Семестр: 4	*Семінарські заняття*:	
	-	-
Тижневе навантаження (год.): - аудиторне: - самостійна робота:	*Консультації:*	
	Індивідуальні заняття:	
Форма підсумкового контролю: залік	-	
Мова навчання: українська	*Самостійна робота:*	
	72	*108*

2. МЕТА ДИСЦИПЛІНИ

Предмет вивчення навчальної дисципліни є процеси, методи та засоби технічного та криптографічного захисту інформації.

Метою вивчення дисципліни «Інформаційні системи та захист інформації» є формування у майбутніх фахівців умінь та компетенцій для забезпечення ефективного захисту інформації, необхідних для подальшої роботи у органах внутрішніх справ та навчити їх застосуванню методів та засобів захисту інформації в умовах широкого використання сучасних інформаційних технологій.

Передумови для вивчення дисципліни «Інформаційна безпека та захист інформації»: 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, сберігання паролів та автентіфікація користувачів в операційних системах.

Міждисциплінарні зв’язки «Основи програмування та алгоритмічні мові», «Архітектура комп’ютера», «Комп’ютерна схемотехніка», «Методи і

засоби комп’ютерних інформаційних технологій», «Технічні засоби передачі інформації», «Комп’ютерні мережі»

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У результаті вивчення навчальної дисципліни студент повинен набути такі результати навчання:

1. *Знання:* правових та організаційних основ забезпечення інформаційної безпеки України та, зокрема, органів внутрішніх справ; основних видів загроз інформаційній безпеці та технічних каналів витоку інформації, методи їх виявлення та блокування; основних видів та можливості технічних засобів і систем захисту інформації; основних методів та засобів криптографічного та стеганографічного захисту інформації, що циркулює у автоматизованих системах ОВС України та передаються телекомунікаційними каналами та мережами.
2. *Уміння:* планувати та організовувати свою роботу та роботу підрозділу з урахуванням вимог до захисту інформації з обмеженим доступом; планувати й організовувати роботи щодо створення та розвитку системи інформаційної безпеки підрозділів органів внутрішніх справ; організовувати роботи щодо виявлення і блокування технічних каналів витоку інформації; здійснювати ефективний контроль робіт із захисту інформації; здійснювати ефективний вибір комп’ютерних систем захисту; свідомо дотримуватися правил роботи з інформацією з обмеженим доступом та сурово виконувати вимоги до захисту інформації, що діють у системі ОВС України; використовувати спеціальні технічні засоби захисту інформації; використовувати програмні та апаратні засоби розмежування доступу до інформації у автоматизованих системах та антивірусні засоби захисту інформації у персональних комп’ютерах; використовувати комп’ютерні криптографічні, стеганографічні системи захисту інформації.
3. *Комунікація:* організовує співпрацю учнів і вихованців та ефективно працює в команді (педагогічному колективі освітнього закладу, інших професійних об’єднаннях).

4. *Автономність та відповідальність:* здатний вчитися упродовж життя і вдосконалювати з високим рівнем автономності здобуті під час навчання компетентності; усвідомлює соціальну значущість майбутньої професії, сформованість мотивації до здійснення професійної діяльності; відповідально ставиться до забезпечення охорони життя і здоров'я учнів у навчально – виховному процесі та позаурочній діяльності.

4. ТЕМАТИЧНИЙ ПЛАН ДИСЦИПЛІНИ

№ з/п	Назви модулів / тем	Кількість годин (денна форма навчання)							Кількість годин (заочна форма навчання)						
		Аудиторні	Лекції	Семінарські (практичні)	Лабораторні	Консультації	Індивідуальні заняття	Самостійна робота	Аудиторні	Лекції	Семінарські (практичні)	Лабораторні	Консультації	Індивідуальні заняття	Самостійна робота
1.	Концептуальні засади забезпечення інформаційної безпеки України	4	2	-	2			8		2		-			10
2.	Технічні канали витоку інформації. Способи несанкціонованого зняття інформаці	4	2		2			8				2			12
3.	Методи та засоби блокування технічних каналів витоку інформації	8	4		4			8		2		2			12
4.	Основи безпеки даних в комп'ютерних системах	8	4		4			10				-			16
5.	Ідентифікація і аутентифікація користувачів	10	4		6			10		2		2			18
6.	Основи захисту даних	4	2		2			8							14
7.	Основи криптографії	8	4		4			8		2		2			12
8.	Стандарти із захисту інформації	4	2	-	2			8							10
Проміжний контроль								4							4
Разом:		48	22	-	26			72		4		8			108

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1. Зміст навчальної дисципліни за темами

Тема 1. Концептуальні засади забезпечення інформаційної безпеки України

Завдання курсу. Нормативно-правові основи захисту інформації в Україні. Концепція національної безпеки України, концепція інформаційної безпеки України, доктрина інформаційної безпеки України. Основні поняття, терміни та визначення. Організація захисту інформації у ОВС України.

Тема 2. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації

Місце технічного захисту інформації у системі інформаційної безпеки. Сутність та завдання технічного захисту інформації. Основні поняття, терміни та визначення технічного захисту інформації. Види інформації, яка може стати об’єктом злочинних посягань. Поняття технічних каналів витоку інформації та механізм їх утворення. Види та класифікація технічних каналів витоку інформації та способів несанкціонованого зняття інформації. Визначення можливих джерел витоку акустичної та електромагнітної інформації у приміщенні. Визначення можливих джерел витоку інформації з радіоканалу.

Тема 3. Методи та засоби блокування технічних каналів витоку інформації

Порядок проведення та складові ТЗІ у підрозділах ОВС України. Методи пасивного та активного захисту інформації. Методи та засоби захисту акустичної інформації. Методи та засіб захисту електромагнітної інформації. Методи захисту від ВЧ-нав’язування. Методики і засоби пошуку радіозакладних пристроїв.

Тема 4. Основи безпеки даних в комп'ютерних системах

Основні поняття щодо захисту інформації в автоматизованих системах. Загрози безпеки даних та їх особливості. Канали проникнення та принципи побудови систем захисту. Основи фізичного захисту об'єктів.

Тема 5. Ідентифікація і аутентифікація користувачів

Поняття про ідентифікацію користувача та її особливості. Основні принципи та методи аутентифікації.

Тема 6. Основи захисту даних

Захист даних від несанкціонованого доступу (НСД). Основні принципи захисту даних від НСД. Моделі управління доступом. Технічні можливості зловмисника і засоби знімання інформації. Технічні засоби захисту даних від їх витоку. Захист даних від комп'ютерних вірусів. Шкідливі програми на ЕОМ. Засоби захисту від комп'ютерних вірусів та їх особливості.

Тема 7. Основи криптографії

Основні терміни та поняття. Криптографічні методи захисту інформації. Сучасні криптосистеми та їх особливості. Класичні техніки шифрування. Симетричні та асиметричні алгоритми шифрування інформації. Цифрові підписи. Адміністрування ключами.

Тема 8. Стандарти із захисту інформації

Світові стандарти із захисту даних в комп'ютерних системах. Державний стандарт України із захисту інформації.

5.2. Тематика лабораторних занять

№	*Теми лабораторних робіт*
1.	Аналіз інформаційної безпеки в Україні.
2.	Програмна реалізація і криптоаналіз шифрів з симетричними ключами.
3.	Основи сучасної криптології. Шифр зсуву; шифр частоколу; шифр одноразового блокноту.
4.	Класичні методи шифрування.
5.	Шифрування за допомогою аналітичних перетворень.
6.	Засоби забезпечення безпеки ОС Windows
7.	Ідентифікація і аутентифікація користувача
8.	Захист об'єктів системі
9.	Алгоритм RSA.
10.	Модифікація шифру Віженера та загального шифру перестановки.
11.	Криптоаналіз лінійних шифрів к-го порядку з відомим відкритим текстом.
12.	Криптоаналіз деяких шифрів з таємним ключем.
13.	Афінні шифри.

5.3. Організація самостійної роботи студентів.

№ з/п	Вид роботи	Кількість годин		Форми звітності
		Денна	Заочна	
1.	Опрацювання лекційного матеріалу.	7	10	Конспект, усна доповідь
2.	Підготовка до лабораторних занять.	13	24	Участь у лабораторних заняттях
3.	Підготовка до модульного контролю.	4	6	Написання МКР.
4.	Підготовка та написання рефератів.	10	16	Реферат.
5.	Робота з інтернет ресурсами.	2	5	Конспект, доповідь
6.	Виконання індивідуального завдання: розв’язування та виконання завдань.	36	47	Демонстрація виконаного завдання у електронному вигляді.
	Разом	**72**	**108**	

Теми рефератів

1. Поняття і класифікація видів та методів несанкціонованого доступу.
2. Визначення і модель зловмисника
3. Організація захисту інформації.
4. Класифікація способів захисту інформації в комп'ютерних системах
5. Фізичні методи захисту інформації
6. Законодавчі методи захисту інформації
7. Управління доступом
8. Криптографічні методи захисту інформації
9. Види умисних загроз безпеки інформації

10. Безпека оптоволоконних кабельних систем
11. Особливості слабкострумових ліній і мереж як каналів просочування інформації
12. Приховування інформації криптографічним методом

Робота з Інтернет-ресурсами

1. Локазюк В.М. , Савченко Ю.Г. Надійність, контроль, діагностика і модернізація ПК –
   Он-лайн підручник - http://www.otk.od.ua/book/index.html
2. Таненбаум Э. Архитектура комп'ютера. – Питер, 2007 – 848 с. - http://mirknig.com/2007/10/24/arkhitektura_kompjutera.html
3. Журнал "CHIP" - Адрес: http://ichip.ru/
4. Журнал " "Мир ПК" - Адрес: http://www.pcworld.ru/
5. Журнал " Мобильные Компьютеры " - Адрес: http://www.mconline.ru/
6. Журнал "Компьютерра" - Адрес: http://www.computerra.ru/
7. Журнал "Железо" - Адрес: http://www.xard.ru/
8. Український щотижневик "Мій комп'ютер" - http://mycomputer.ua/

Індивідуальне завдання

Пропонується виконати послідовність дій, яку необхідно періодично проводити на кожному робочому місці, обладнаному ПК для попередження втрат інформації внаслідок проникнення вірусів, троянських програм чи некваліфікованих користувачів.

1. ***Контроль за віросуподібними змінами.***

Перевірити час і дату. В OS MS DOS це можна зробити командами Data і Time. Однією з причин неправильних показів системного годинника може бути діяльність вірусів.

Уточнити версію операційної систми командою. Порівняти довжину і час створення системних файлів на різних комп'ютерах з однаковими версіями.

Скласти таблицю довжин для системних та EXE- файлів, встановлених на даному комп'ютері. Зміна довжин чи часу і дати цих файлів з великою ймовірністю свідчить про появу вірусів.

2. ***Перевірка всіх дисків антивірусними програмами.***

Познайомитися з антивірусними програмами, встановлених на даному комп'ютері. Звернути увагу на дату їх написання. Перевірити всі флешки і розділи жорсткого диска діагностичними програмами.

Встановити одну з нових версій антивірусних програм або додаткові інформаційні файли для вже встановленої. Підготувати коротку вичерпну інструкцію для користувачів.

3. ***Перевірка файлової структури всіх розділів жорстких дисків.***

Познайомитися з програмою ScanDisk і NortonDiskDoctor, з допомогою яких виявляють і виправляють помилки в каталогах і таблицях розміщення файлів на флешках і жорстких дисках.

4. ***Підготовка системного та рятівного дисків.***

Підготувати системну флешку, записати декілька антивірусних програм, захистити від запису і тримати в надійному місці для можливого використання у випадку зараження комп'ютера вірусами чи пошкодження системних файлів на вінчестері.

З допомого утиліти Rescue підготувати аварійний компакт-диск для кожного комп'ютера з важливою системною інформацією, яка дає можливість відновити файлову структуру після руйнівної дії вірусів чи краху системи з інших причин (вимкнення напруги, випадкове знащення).

5. **Профілактика макро-вірусів.**

Якщо на комп'ютері встановлений текстовий редактор Word, перевірити яка захисна система для нього встановлена. При можливості встановити більш нову версію, викликаючи документ-імунізатор типу Avpww.doc або Drwebww.doc.

6. ФОРМИ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

6.1. Форми поточного контролю: перевірка виконання завдань для самостійної роботи, перевірка виконання завдань під час лабораторних робіт
6.2. Форми проміжного контролю: модульна контрольна робота.
6.3. Форми підсумкового контролю: залік.

7. ЗАСОБИ ДІАГНОСТИКИ РЕЗУЛЬТАТІВ НАВЧАННЯ

У якості діагностики результатів навчання проводиться модульна контрольна робота у письмовій формі. Критерії оцінювання висвітлені у розділі 8.5. *Критерії оцінювання модульної контрольної роботи.*

Приклад модульної контрольної роботи

1. Проблема захисту інформації шляхом її перетворення.
2. Абстрактні моделі захисту інформації.

3. Які програмні продукти застосовуються для пошуку паролів?
4. Особливості програми Windows Disk Wiper.
5. Порядок установлення, зняття пароля облікового запису користувача у програмі MS Access.

8. КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

8.1. Шкала та критерії оцінювання знань студентів.

Оцінювання знань студентів відбувається відповідно до «Положення про порядок оцінювання рівня навчальних досягнень здобувачів вищої освіти в умовах ЄКТС» (ІДГУ, 2018) із урахуванням ***вагових коефіцієнтів***:

– **поточного контролю -** 0,7;
– **проміжного контролю** – 0,3;

Переведення підсумкового балу за 100-бальною шкалою оцінювання в підсумкову оцінку за традиційною шкалою

Підсумковий бал	Оцінка за традиційною шкалою
90-100	зараховано
70-89	
51-69	
26-50	не зараховано

8.2. Критерії оцінювання під час аудиторних занять

Оцінка	Критерії оцінювання навчальних досягнень
5 балів («відмінно»)	Оцінюється робота студента, який у повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає, глибоко та всебічно розкриває зміст *теоретичних запитань* та *практичних завдань*. Використовуючи при цьому обов'язкову та додаткову літературу, вільно послуговується науковою термінологією, розв'язує завдання стандартним або оригінальним способом, наводить аргументи на підтвердження власних думок, здійснює аналіз та робить висновки.
4 бали («добре»)	Оцінюється робота студента, який достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає, в основному розкриває зміст теоретичних запитань та *практичних завдань*. Але при висвітленні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі неістотні неточності та незначні помилки.
3 бали («задовільно»)	Оцінюється робота студента, який відтворює значну частину навчального матеріалу, висвітлює його основний зміст, виявляє елементарні знання окремих положень. Виконує практичні завдання. Не здатний до глибокого, всебічного аналізу, обґрунтування та аргументації, не користується необхідною літературою, допускає істотні неточності та помилки.
2 бали («незадовільно»)	Оцінюється робота студента, який не володіє навчальним матеріалом у достатньому обсязі, проте фрагментарно, поверхово (без аргументації та обґрунтування) викладає окремі питання навчальної дисципліни, не розкриває зміст теоретичних питань і практичних завдань.

1 бал («початковий рівень»)	Оцінюється робота студента, який не в змозі викласти зміст більшості питань теми та курсу, володіє навчальним матеріалом на рівні розпізнавання явищ, допускає істотні помилки, відповідає на запитання, що потребують однослівної відповіді.
0 балів («низький рівень»)	Оцінюється робота студента, який не володіє навчальним матеріалом та не в змозі його висвітлити, не розуміє змісту теоретичних питань та практичних завдань.

8.3. Критерії оцінювання індивідуальних завдань

Критеріями оцінювання індивідуальних завдань студента є:

1. самостійність виконання завдання;
2. правильність, точність, оптимальність реалізації поставленого завдання;
3. завершеність завдання.
4. вміння захищати результати проведеного дослідження.

Оцінка	Критерії оцінювання індивідуальних завдань
5 балів	Оцінюється робота студента, який вільно володіє матеріалом розробленого проекту, творче його осмислив, оперує поняттями та категоріями, вміє встановити зв'язок між теоретичною базою та практикою, залучає до відповіді самостійно опрацьовану літературу. Відповідає на додаткові запитання, наводить аргументи на підтвердження власних думок, здійснює аналіз та робить висновки. Презентація відповідає наступним вимогам: послідовність, інформативність матеріалу, цілісність, відеоряд.
4 бали	Оцінюється робота студента, який достатньо повно володіє матеріалом розробленого проекту, орієнтується в ньому, оперує необхідним колом понять та категорій щодо проекту, вміє встановити зв'язок між теоретичною базою та практикою. Відповідь з незначною кількістю помилок, відповідає на додаткові запитання, але не має аргументованої думки, висновки не повні. Презентація частково відповідає наступним вимогам: послідовність, інформативність матеріалу, цілісність, відеоряд.
3 бали	Оцінюється робота студента, який виконав проект який містить значну кількість недоліків і помилок, неповне висвітлення змісту питань володіє матеріалом і частково відповідає на додаткові питання, недостатньо відповідає на питання, не може зробити аргументовані висновки. Презентація частково відповідає наступним вимогам: послідовність, інформативність матеріалу, цілісність, відеоряд.
2 бали	Проект виконано не правильно, студень показує істотне нерозуміння проблеми, в роботі не виконано всі завдання; або студент не здатен захистити результати поданого проекту
1 бали	Проект відзначається фрагментарністю, студень показує істотне нерозуміння проблеми, в роботі не виконано всі завдання; однак студент володіє умінням здійснювати первинну обробку навчальної інформації без подальшого її аналізу
0 балів	Оцінюється робота студента, який не виконав індивідуальне завдання

Критерії оцінювання реферату

Оцінка	Критерії оцінювання реферату
5 балів	Виконано всі вимоги до написання й захисту реферату: позначені проблема й обґрунтована її актуальність, зроблено аналіз різних точок зору на проблему й логічно викладено власна позиція, тема розкрита повністю, сформульовано висновки, витримано обсяг роботи, дотримано вимоги до

	оформлення, подано правильні відповіді на питання по змісту реферату
4 бали	Виконано основні вимоги до реферату, але допущено деякі недоліки: проблема позначена, але не достатньо обґрунтована її актуальність, зроблено короткий аналіз різних точок зору на проблему, але не викладено власна позиція, сформульовано висновки, але не достатньо узагальнено, подано правильні відповіді по змісту реферату, дотримано вимоги до оформлення
3 бали	Основні вимоги до реферату і його захисту виконано, але є істотні відступи від вимог до реферування, зокрема: тема розкрита лише частково, допущено фактичні помилки в змісті, відсутня логічна послідовність у судженнях, відсутні висновки; не витримано обсяг реферату, є недоліки в оформленні; на додаткові питання при захисті подано не повні відповіді
2 бали	Тема реферату не розкрита, студень показує істотне нерозуміння проблеми, не витримано обсяг реферату; є недоліки в оформленні; на додаткові питання при захисті подано не правильні відповіді або не дано зовсім
1 бал	Проведена робота, однак тема реферату не відповідає змісту, план – темі і змісту, не дотримано вимог до оформлення і літератури, при відповіді на питання не розуміє сутність теми
0 балів	Реферат не написано

Критеріями оцінювання реферату студента є:

Новизна змісту:

а) самостійність у формулювання нового аспекту відомої проблеми, встановленні нових зв'язків (міжпредметних, внутрішнь-опредметних, інтеграційних);

б) уміння працювати з дослідженнями, аналітичною літературою, систематизувати й структурувати матеріал;

в) наявність авторської позиції, самостійність оцінок і суджень.

Ступінь розкриття сутності питання:

а) відповідність плану й змісту реферату його темі;

б) повнота й глибина знань з теми;

в) обґрунтованість способів і методів роботи з матеріалом;

г) уміння узагальнювати, робити висновки, зіставляти різні точки зору по одному питанню (проблемі).

Оцінка використаної літератури: чи розглянуті найбільш відомі роботи з теми дослідження (у т.ч. журнальні публікації останніх років, останні статистичні дані тощо).

Дотримання вимог до оформлення:

а) правильність оформлення посилання на використану літературу, список літератури;

б) оцінка грамотності й культури викладу, володіння термінологією;

в) дотримання вимог до обсягу реферату.

8.4. Критерії оцінювання модульної контрольної роботи

Кожне питання оцінюється у 5 бальній шкалі, виводиться середнє значення за 5 питань.

Критерії оцінювання МКР	
26-30 балів – «відмінно»	Студент має систематичні та глибокі знання, викладає матеріал у логічній послідовності, робить узагальнення й висновки, наводить практичні приклади у контексті теоретичного матеріалу, вміє без

	помилок виконувати практичні завдання, які передбачені програмою курсу.
21-25 балів – «добре»	Студент повністю засвоїв учбовий матеріал, вміє виконувати практичні завдання, викладає матеріал у логічній послідовності, робить певні узагальнення й висновки, але не наводить практичних прикладів у контексті викладеного матеріалу або допускає незначні помилки у формулюванні термінів, категорій, невеликі помилки у розрахунках при вирішенні практичних завдань.
16-20 балів – «задовільно»	Студент засвоїв матеріал не у повному обсязі, дає не повну відповідь на поставлені теоретичні питання, допускається грубих помилок при розв‘язанні практичного завдання.
1-15 балів – «незадовільно»	Студент не засвоїв учбовий матеріал, дає неправильні відповіді на поставлені теоретичні питання, не вміє або неправильно виконує розрахунки при розв‘язанні практичних завдань.

8.5. Критерії оцінювання під час підсумкового контролю.

Підсумкова оцінка виставляється за результатами поточного та проміжного контролю.

9. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Викладання дисципліни (проведення лекцій і лабораторних занять) передбачає аудиторію з мультимедійною дошкою або мультипроектором, комп’ютерами з вільним доступом до Інтернет. Кількість робочих станцій має відповідати кількості студентів у підгрупі.

14.РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

10.1. Основні джерела

1. Рибальський О.В. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України / Рибальський О.В., Смаглюк В.М., Хахановський В.Г. – К.: НАВС, 2013. – 255 с.
2. Коженевський С.Р. Термінологічний довідник з питань захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков. – К.: ДУІКТ, 2007. – 382 с.
3. Рибальський О.В. Захист інформації в інформаційно-комунікаційних системах. Навчальний посібник для курсантів ВНЗ МВС України / О.В. Рибальський, В.Г. Хахановський, В.А. Кудінов, В.М. Смаглюк. – К.: Вид. Національної академії внутріш. справ, 2013. – 118 с.
4. Каторин О.Ф. Большая энциклопедия промышленного шпионажа / О.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко. – С.Пб.: ООО "Издательство Полигон", 2000. – 896 с.
5. С. Синх. Книга кодов. Тайная история кодов и их “взлома” / С. Синх. – М.: ООО “Издательство Астель”, 2007. – 447 с.
6. Хорошко В.О. Основи комп’ютерної стеганографії / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця.: ВДТУ, 2003. – 142 с.
7. Наказ МВС України від 14.07.1998 р. “Про організацію і виконання робіт з технічного захисту інформації з обмеженим доступом в системі МВС України”. – К., 1998.

8. Наказ МВС України № 59 від 14.06.98 р. “Про організацію та виконання робіт з технічного захисту інформації з обмеженим доступом в системі МВС України”.

9. Закон України “Про державну таємницю” від 21.01.1994 // Відомості Верховної Ради України, 1994, № 16. – Ст. 93.

10.Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.

11. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 // Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2005 р.

12.Закон України “Про телекомунікації” від 18.11.2003 // Відомості Верховної Ради України, 2004, № 12. – Ст. 155, із змінами 2004 р.

13.Постанова Кабінету Міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” від 08.10.1997 р.

14.Постанова Кабінету Міністрів України “Про затвердження Положення про технічний захист інформації в Україні” від 09.09.1994 р.

15.Постанова Кабінету міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” № 1126 від 08.11.1997 р.

10.2. Допоміжні джерела

1. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.

2. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

3. Максименко Г.А. Методы выявления, обработки и идентификации сигналов радиозакладных устройств / Максименко Г.А., Хорошко В.А. – К.: ООО «ПолиграфКонсалтинг», 2004. – 317 с.

4. ДСанПіН 3.3.6.096-2002 Державні санітарні норми і правила при роботі з джерелами електромагнітних полів

5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

6. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт.

10.3. Інтернет-ресурси

1. Локазюк В.М. , Савченко Ю.Г. Надійність, контроль, діагностика і модернізація ПК –
   Он-лайн підручник - http://www.otk.od.ua/book/index.html
2. Таненбаум Э. Архитектура комп’ютера. – Питер, 2007 – 848 с. - http://mirknig.com/2007/10/24/arkhitektura_kompjutera.html
3. Журнал "CHIP" - Адрес: http://ichip.ru/
4. Журнал " "Мир ПК" - Адрес: http://www.pcworld.ru/
5. Журнал " Мобильные Компьютеры " - Адрес: http://www.mconline.ru/
6. Журнал "Компьютерра" - Адрес: http://www.computerra.ru/
7. Журнал "Железо" - Адрес: http://www.xard.ru/
8. Український щотижневик "Мій комп'ютер" - http://mycomputer.ua/