Уманський державний педагогічний університет імені Павла Тичини
Факультет фізики, математики та інформатики
Кафедра інформатики і інформаційно-комунікаційних технологій

«ЗАТВЕРДЖУЮ»

Завідувач кафедри
_____ М.О. Медведєва
8 серпня 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ВВ 1.04 БЕЗПЕКА КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Галузь знань 01 Освіта / Педагогіка

Спеціальність 014.09 Середня освіта (Інформатика)

Освітня програма Середня освіта (Інформатика)

Умань – 2022

Робоча програма з безпеки комп'ютерних систем та мереж для студентів спеціальності 014.09 Середня освіта (Інформатика).

Розробник: Бондаренко Тетяна Володимирівна, доцент кафедри інформатики і інформаційно-комунікаційних технологій, кандидат педагогічних наук

Робочу програму схвалено на засіданні кафедри інформатики і інформаційно-комунікаційних технологій.

Протокол №1 від 8 серпня 2022 року.

Завідувач кафедри інформатики і інформаційно-комунікаційних технологій

_____ _____(Медведєва М.О.)
(підпис) (прізвище та ініціали)

Робочу програму розглянуто та затверджено на засіданні науково-методичної комісії факультету фізики, математики та інформатики

Протокол № 1 від «8» серпня 2022 року

Голова науково-методичної комісії факультету фізики, математики та інформатики

_____ Тягай І.М.
(підпис) (прізвище та ініціали)

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 чи вибіркова)	вибіркова	вибіркова
Мова викладання, навчання та оцінювання	українська	українська
Загальний обсяг у кредитах ЄКТС / годинах	4/120	4/120
Курс	4	4
Семестр	8	8
Кількість змістових модулів із розподілом:	2	2
Обсяг кредитів	4	4
Обсяг годин, у тому числі:	120	120
Аудиторні:	54	12
Лекційні	20	4
Семінарські / Практичні		
Лабораторні	34	8
Самостійна робота	66	108
Індивідуальні завдання	ІНДЗ	ІНДЗ
Форма семестрового контролю	Екзамен	Екзамен

2. Мета та завдання навчальної дисципліни

Мета курсу: формування умінь та компетенцій для забезпечення безпеки комп'ютерних систем та мереж, необхідних для подальшої роботи; застосування методів та засобів захисту як окремих вузлів, так і комп'ютерної мережі в цілому, від зовнішнього та внутрішнього втручання.

Завдання:

Основні завдання, на вирішення яких спрямована дисципліна: навчити виявляти, ставити та вирішувати проблеми за професійним спрямуванням; сформувати здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки; сформувати здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.); сформувати здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

3. Результати навчання за дисципліною

Вивчення дисципліни має на меті сформувати наступні загальні і фахові компетентності та отримати такі програмні результати навчання як:

ІК: Здатність розв'язувати складні спеціалізовані теоретичні та практичні завдання в галузі середньої освіти, педагогіки та інформаційних технологій, що передбачає застосування концептуальних методів освітніх наук, теорії та методики навчання інформатики і характеризуються комплексністю та невизначеністю умов організації освітнього процесу в закладах загальної середньої освіти (базова середня освіта).

ЗК 2: Здатність до міжособистісної взаємодії, роботи в команді, спілкування з представниками інших професійних груп різного рівня (соціальна компетентність).

ПК 3: Інформаційно-цифрова компетентність як здатність: орієнтуватися в інформаційному просторі, здійснювати пошук і критично оцінювати інформацію, оперувати нею у професійні і й діяльності; ефективно використовувати наявні та створювати (за погреби) нові електронні (цифрові) освітні ресурси; використовувати

цифрові технології в освітньому процесі.

ПК 14: Здатність до навчання впродовж життя як здатність: визначати умови та ресурси професійного розвитку впродовж життя; взаємодіяти з іншими вчителями на засадах партнерства та підтримки (у рамках наставництва, супервізії тощо).

ПРН1: Знає основні історичні етапи розвитку предметної галузі.

ПРН4: Знає та розуміє структуру предметної галузі, місце інформатики в системі наук, розуміє перспективи розвитку інформаційно-комунікаційних технологій та їхнє суспільне значення.

ПРН5: Знає та розуміє фізичні, логічні та математичні основи інформатики та інформаційно-комунікаційних технологій.

ПРН8: Оперує базовими категоріями та поняттями предметної галузі, в тому числі загальноприйнятою міжнародною ІТ-термінологією.

ПРН9: Застосовує знання нормативно-правових документів та міжнародних й національних стандартів для ефективної організації професійної та громадської діяльності.

ПРН14: Володіє прийомами, методами та засобами ефективного пошуку інформації, критичного аналізу та опрацювання даних для використання у професійній діяльності з дотримання принципів академічної доброчесності.

ПРН15: Вміє використовувати та добирати засоби ІКТ для розв'язання конкретних задач у професійній діяльності (проєктування інформаційно-освітнього середовища та його окремих компонент, створення програмних засобів, розробки вебресурсів тощо).

ПРН20: Здатний самостійно приймати рішення на основі сформованих ціннісних орієнтирів та моральної автономії, що дозволяє, зберігаючи людську гідність і доброчесність, бути вільним від зовнішнього тиску, диктату влади, усталених норм, думки інших.

4. Програма навчальної дисципліни

Змістовий модуль 1. Безпека глобальних мереж та серверів

Тема 1. Основи безпеки Internet.

Internet і безпека. Організація IANA, RIR, LIR, AS та захист розподілу IP-адрес. Кореневі DNS та правила розподілу і функціонування доменних імен. Безпека рівнів TCP/IP. Захист на рівнях моделі відкритих систем OSI/ISO.

Тема 2. Стандарти та групи та класи захисту комп'ютерних мереж.

Стандарти оцінювання захисту. Критерії оцінювання захищених комп'ютерних систем Міністерства оборони США (TCSEC). Європейські критерії безпеки інформаційних технологій (ITSEC). Федеральні критерії безпеки інформаційних технологій США (FCITS). ISO/IEC 15408-Common Criteria. Нормативні документи системи технічного захисту інформації України (НД ТЗІ)

Тема 3. Рівні безпеки комп'ютерних мереж.

Законодавчий рівень. Адміністративний рівень. Засоби безпеки процедурного рівня. Засоби безпеки технічного рівня. Політики безпеки.

Тема 4. Безпека операційних систем серверів та мейнфремів.

Еволюція безпеки ОС (UNIVAC, CTTS, ITSS, Atlas, VMS, THE, RS4000, DOS). Захист в сімействі Windows (3.1, NT, 95, OS/2, 98, ME, 2000, XP, 2003, Vista, 7, 2008, 2012, 2016, 10, 2020).Безпека Unix-подібних ОС (AIX, HP-UX, IRIX, SCO-UX, SunOS, Solaris, BSD, FreeBSD, Linux). Засоби захисту сімейства MAC-OS. Операційні системи мейнфреймів та безпека (B5000, IBM System/360, UNIVAC 1108).

Тема 5. Основи захисту серверів ОС Windows.

Аутентифікація користувачів в серверах ОС Windows. Доступ на основі ресурсів серверів ОС Windows Управління доступом в операційних системах Windows на основі Active Directory. Централізовані системи аутентифікації і авторизації LDAP.

Тема 6. Засоби захисту UNIX-подібних систем (зокрема, Linux).

Аутентифікація в ОС сімейства Unix. Права груп і користувачів до файлів. Концепція єдиного логічного входу NIS. Система LDAP. Система Kerberos. Протокол SSH.

Змістовий модуль 2. Безпека інфраструктури та IP-мереж

Тема 7. Безпека фізичного рівня та кабельної інфраструктури.

Захист консольного доступу пристроїв та комп'ютерів. Безпека кабелів на основі міді. Волоконнооптичні кабелі та їх безпека. Захист в бездротових комп'ютерних мережах Wi-Fi. Захист мобільного зв'язку. Супутниковий зв'язок і його безпека. Пасивне мережеве обладнання

Тема 8. Безпека канального рівня.

Активне мережеве обладнання і його захист. Повторювачі (Repeater). Концентратори (Hub). Мости (Bridge). Комутатори (Switch). Точки доступу (Access Point). Шлюз (Gateway). Фільтрація мережевих кадрів. Сегментація фізичних мереж. ARP-spoofing. Віртуальні локальні мережі VLAN. Протокол PPPoE. Віртуальні канали MPLS.

Тема 9. Фільтрація і моніторинг IP-трафіку.

Фільтрація. Види фільтрації. Стандартні і додаткові правила фільтрації маршрутизаторів. Типи фаєрволів. Фільтруючі маршрутизатори. Брандмауери та екрани. Пристрої UTM. Апаратні файєрволи. IDP-сигнатури атак. Системи детектування атак.

Тема 10. Поняття трансляції IP-адрес NAT.

Технологія NAT. Технологія SAT, PAT та Masqurade. IP-адреси для внутрішнього використання intarnet. Базова трансляція IP-адрес. Трансляція мережевих портів. Фаєрволи з функцією NAT. Програмні фаєрволи хоста.

Тема 11. Проксі-сервери.

Поняття кешуючих серверів. Проксі-сервери Лінукс. Проксі-сервери Windows. Наскрізний transparent-proxy. Конфігурування кешуючих серверів.

Тема 12. ICMP та IP-атаки мережевого рівня.

ICMP-атаки. Перенаправлення трафіку. ICMP-атака Smurf. ICMP-затоплення. Пінг смерті і ping-затоплення. Echo/chargen-затоплення. IP-атаки. Атака на IP-опції. IP-атака на фрагментацію.

Тема 13. Атаки на протоколи граничної маршрутизації.

Безпека маршрутизації на основі BGP. Уразливості і інциденти протоколу BGP. Маніпуляції з маршрутними оголошеннями. Захист BGP. Захист BGP-маршрутизації на основі бази даних маршрутів. Сертифікати ресурсів і їх використання для захисту BGP.

Змістовий модуль 3. Захист транспортних з'єднань та прикладних служб

Тема 14. Атаки на транспортний та сеансовий рівні TCP/ UDP.

UDP-атаки. UDP-затоплення. TCP-атаки. Затоплення SYN-пакетами Підробка TCPсегмента. Скидання TCP-з'єднання.

Тема 15. Безпека протоколів прикладного рівня.

Протоколи HTTP, FTP, SMTP, POP3, IMAP4v1, SNMP, Telnet. Протокол передачі гіпертексту HTTP. Протокол передачі файлів FTP. Простий протокол передачі пошти SMTP. Протокол отримання електронної пошти POP3. Протокол доступу до повідомлень мережі Інтернет IMAP4v1. Спам. Простий протокол керування мережевими пристроями SNMP. Протокол віддаленого доступу Telnet.

Тема 16. Сертифікати SSL та безпечні прикладні протоколи SSH і HTTPS.

Характеристики протоколу SSL. Ієрархія ключів та сертифікатів. Цифровий підпис даних в мережі. Протокол віддаленого доступу SSH. Протокол передачі гіпертексту HTTPS.

Тема 17. Атаки на доменні імена.

Атаки на DNS. DNS-спуффінг. Отруєння кеша DNS. Атаки на кореневі DNS-сервери. DDoS-атаки відображенням від DNS-серверів. Методи захисту служби DNS.

Тема 18. Сканери мереж.

Сканування мережі. Сканування портів. Виявлення мережевих сервісів та їх версій. Мережева розвідка. Виявлення версії операційної системи пристрою чи комп'ютера. Атаки на мережеві сервіси протоколів прикладного рівня. Сканер NMAP.

Тема 19. Моніторинг та виявлення атак.

Моніторинг трафіку. Аналізатори протоколів. Система моніторингу NetFlow та JFlow. Системи виявлення вторгнень. Система SNORTD. Архітектура мережі з захистом периметра. Мережі із поділом внутрішніх зон.

Тема 20. Віртуальні приватні мережі VPN.

Способи створення захищеного каналу. Транспортний і тунельний режими. Ієрархія технологій захищеного каналу. VPN на основі шифрування. Протокол PPTP. Розподіл функцій між протоколами IPSec. Український стандарт симетричного шифрування «Калина». Світовий стандарт симетричного шифрування AES.

5. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Модуль 1												
Змістовий модуль 1 Безпека глобальних мереж та серверів												
Тема 1. Основи безпеки Internet.	**5**	1		1		3	**5**					5
Тема 2. Стандарти, групи та класи захисту комп'ютерних мереж.	**5**	1		1		3	**5**					5
Тема 3. Рівні безпеки комп'ютерних мереж.	**6**	1		2		3	**6**	1		2		3
Тема 4. Безпека операційних систем серверів та мейнфремів.	**6**	1		2		3	**6**					6
Тема 5. Основи захисту серверів ОС Windows.	**6**	1		2		3	**6**	1				5
Тема 6. Засоби захисту UNIX-подібних систем (зокрема, Linux).	**6**	1		2		3	**6**					6
Разом за змістовим модулем 1	**34**	**6**		**10**		**18**	**34**	**2**		**2**		**30**
Змістовий модуль 2 Безпека інфраструктури та IP-мереж												
Тема 7. Безпека фізичного рівня та кабельної інфраструктури.	**5**	1		1		3	**5**					5
Тема 8. Безпека канального рівня.	**5**	1		1		3	**5**					5
Тема 9. Фільтрація і моніторинг IP-трафіку.	**6**	1		2		3	**6**					6
Тема 10. Поняття трансляції IP-адрес NAT.	**6**	1		2		3	**6**					6
Тема 11. Проксі-сервери.	**6**	1		2		3	**6**					6
Тема 12. ICMP та IP-атаки мережевого рівня.	**9**	1		2		6	**9**					9
Тема 13. Атаки на протоколи граничної маршрутизації.	**9**	1		2		6	**9**	2		2		5
Разом за змістовим модулем 2	**46**	**7**		**12**		**27**	**46**	**2**		**2**		**42**
Змістовий модуль 3 Захист транспортних з'єднань та прикладних служб												
Тема 14. Атаки на транспортний та сеансовий рівні TCP/ UDP.	**6**	1		2		3	**6**					**6**
Тема 15. Безпека протоколів прикладного рівня.	**6**	1		2		3	**6**			2		**4**
Тема 16. Сертифікати SSL та безпечні прикладні протоколи SSH і HTTPS.	**6**	1		2		3	**6**					**6**
Тема 17. Атаки на доменні імена.	**6**	1		2		3	**6**					**6**
Тема 18. Сканери мереж.	**6**	1		2		3	**6**			2		**4**
Тема 19. Моніторинг та виявлення атак.	**5**	1		1		3	**5**					**5**
Тема 20. Віртуальні приватні мережі VPN.	**5**	1		1		3	**5**					**5**
Разом за змістовим модулем 3	**40**	**7**		**12**		**21**	**40**			**4**		**36**
Усього годин	**120**	**20**		**34**		**66**	**120**	**4**		**8**		**108**

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Вивчення та дослідження приналежності IP-адреси	6
2	Видача доменних імен та їх безпека	6
3	Безпека серверів ОС Windows	4
4	Захист систем ОС Linux	4
5	Система фільтрації трафіку	4
6	Трансляція IP-адрес NAT.	4
7	Проксі-сервер	6
	Всього:	34

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Атаки в віртуальному середовищі	6
2	Технології віртуалізації	6
3	Мережеві загрози у віртуальному середовищі	6
4	Захист віртуального середовища.	6
5	Схема захисту Deep Security	6
6	Захист веб-додатків	6
7	Розмежування прав	6
8	Обмеження управління і політики	6
9	Віртуальні загрози майбутнього	6
10	Організація захисту від вірусів. Способи виявлення вірусів.	6
11	Проблеми антивірусів. Архітектура антивірусного захисту	6
12	Боротьба з небажаною поштою	6
13	Міжмережеві екрани. Принципи роботи міжмережевих екранів	6
14	Апаратні та програмні МЕ. Спеціальні МЕ	6
15	Канали витоку	6
16	Засоби запобігання витокам	6
17	Засоби виявлення і запобігання вторгнень	6
18	Промислові рішення моніторингу подій	6
	Всього:	108

9. Індивідуальні завдання

1. Модель загроз для операційної системи
2. Типова архітектура комплексу засобів захисту операційних систем
3. Порівняльна характеристика підходів до побудови захищених систем
4. Критерії оцінювання захищених комп'ютерних систем Міністерства оборони США (TCSEC)
5. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ)
6. Стандарт ISO 15408: основні документи, структура профілю захисту і завдання з безпеки
7. Стандарт ISO 15408: структура стандарту, основні документи, структура вимог
8. Компоненти КЗЗ ОС Windows. Взаємодія компонентів і БД системи безпеки
9. Підсистема розмежування доступу ОС Windows. Суб’єкти і об’єкти доступу
10. Суб’єкти і об’єкти доступу ОС Windows. Реалізація дискреційного керування доступом

11. Алгоритми з’ясування прав доступу в ОС Windows12. Реалізація підсистеми ідентифікації й автентифікації в ОС Windows
13. Архітектура і модель безпеки системи UNIX. Основні недоліки традиційної моделі безпеки UNIX
14. Підсистема ідентифікації та автентифікації UNIX. Підсистема розмежування доступу
15. PAM-автентифікація в Linux
16. Реалізація мандатного керування доступом і адміністрування безпеки у середовищі Trusted Solaris
17. Security Enhanced Linux: політики, контексти безпеки, операції
18. Процесори Intel i386: структури даних, що пов’язані з розмежуванням доступу до оперативної пам’яті
19. Процесори Intel i386: реалізація кілець захисту; привілейовані і чутливі команди
20. Процесори Intel i386: керування доступом до сегментів пам’яті під час звернень до нового сегмента та звернень за адресою у поточному сегменті
21. Процесори Intel i386: керування викликом процедур і задач
22. Загрози безпеці інформації у комп'ютерних мережах, віддалені атаки
23. ITU-T, рекомендації X.800. Основні сервіси і механізми безпеки в мережах
24. Проблеми протоколу IP і його реалізацій з точки зору безпеки інформації. Основні атаки на IP
25. Проблеми протоколу TCP і його реалізацій з точки зору безпеки інформації. Основні атаки на TCP
26. Безпека DNS. Можливі атаки
27. Протокол ICMP. Можливі атаки. Рекомендації із застосування
28. Проблеми протоколів Telnet і FTP. Уразливості. Методи захисту.
29. Безпека системи електронної пошти.
30. Безпека служби WWW: вразливості клієнтського ПЗ. Підвищення ступеня захищеності клієнтського ПЗ.
31. Безпека служби WWW: вразливості серверного ПЗ. Приклади атак.
32. Безпека CGI-застосунків: ін’єкції, методи захисту.
33. Міжмережні екрани. Класифікація, можливості й обмеження
34. Віртуальні приватні мережі (VPN). Сервіси віртуальних приватних мереж. Типи віртуальних приватних мереж
35. VPN віддаленого доступу. Протоколи PPTP і L2TP
36. VPN мережного рівня. IPsec (протоколи, режими, утворення захищених асоціацій)
37. VPN сеансового рівня: функції посередництва, протоколи
38. Засоби виявлення атак і протидії атакам

10. Методи навчання

В освітньому процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора; лабораторні, групові, індивідуальні, дистанційні форми роботи.

11. Методи контролю

Екзамен, активність на лабораторному занятті, індивідуальне дослідницьке завдання, завдання для самостійної роботи, тестовий контроль, презентація результатів дослідження.

12. Критерії оцінювання

При визначені оцінки знань студентів викладач керується критеріями і положеннями, які розроблені Міністерством освіти і науки України. Крім цього, при оцінюванні засвоєння знань студентів проводиться після вивчення модуля модульний контроль, результати, якого оцінюються за нижче наведеними

критеріями та заносяться в академічний журнал окремим рядком.

Оцінки «відмінно» заслуговують відповіді студентів, що показали глибокі знання програми курсу, засвоїли основну літературу, набули визначеного програмою кола необхідних знань та мають визначені практичні навички. Крім того, враховується вміння грамотно, чітко і послідовно викласти питання, що розглядається. Швидко виконувати поставлені практичні задачі.

Оцінки «добре» заслуговують відповіді студентів, які виявили тверді знання навчального матеріалу в обсязі навчальної програми, не допустили суттєвих помилок при відповіді на всі питання, чітко виклали матеріал та показали здібності і вміння застосовувати одержані знання у своїй практичній діяльності при використанні натяків на виконання практичних завдань.

Оцінки «задовільно» виставляється студентам, які показали знання основного матеріалу в обсязі навчальної програми, але допустили при відповіді помилки, невірність окремих формулювань, положень, або які показали поверхові знання з питань, не чітко і не аргументовано дали відповідь на поставлені запитання. Виконувати лабораторні завдання можуть виконувати лише при додаткових вказівках.

Оцінки «незадовільно» заслуговують відповіді студентів, які показали недостатні знання навчального матеріалу, не знають основних понять та положень дисципліни, не вміють виконувати елементарні практичні завдання і зовсім не орієнтуються в питаннях до лабораторної роботи, чим виявили непридатність до професійної діяльності.

13. Розподіл балів, які отримують студенти

МОДУЛЬ 1																				МК	ІНДЗ	ПК	ВСЬОГО
Змістовий модуль 1						Змістовий модуль 2							Змістовий модуль 3										
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т12	Т13	Т14	Т15	Т16	Т17	Т18	Т19	Т20				
2	2	4	4	4	4	2	2	4	4	4	4	4	4	4	4	4	4	2	2	10	12	10	100

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка за національною шкалою	
	для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100(A)	відмінно	зараховано
82 – 89(B)	добре	
75 –81(C)		
68 – 74(D)	задовільно	
61 – 67(E)		
35 – 60(FX)	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1 – 34(F)	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

14. Рекомендована література

1. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. – 449 с.

2. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. – Житомир: ЖНАЕУ, 2016. – 636 с.

3. Лісовська Ю. Кібербезпека. Ризики та заходи. – К.: Кондор, 2019. – 272 с.

4. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.

5. Антоненко О. Криптографічні методи перетворення інформації: навч. посіб. – Бердянськ: БДПУ, 2015. – 180 с.

6. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf

7. Фергюссон Н., Шнайер Б. Практическая криптография. – М.: ДиалектикаВильямс, 2016. – 420 с.

15. Інформаційні ресурси

http://www.library.kr.ua/libworld/elib.html	Бібліотеки в Інтернет
http://www.nbuv.gov.ua/	Національна бібліотека України ім. Вернадського
http://www.nbuv.gov.ua/libdoc/	Комп’ютерні технології в бібліотеці (Київ)
http://www.nbuv.gov.ua/eb/tp.html	Електронний фонд науковий публікацій (Київ)
http://www.infocity.kiev.ua/	UnfoCiti(Київ)Тексти з комп’ютерних технологій
http://lib.meta.ua	Библиотека на Meta.ua (Харьков)
http://www.utoronto.cf/elul/	Електронна бібліотека української літератури (Канада)
http://www.library.edu-ua.net/	Державна науково-педагогічна бібліотека України імені В. О. Сухомлинського (Київ)
http://www.gntb.n-t/org/	Державна науково-технічна бібліотека України (Київ)
http://www.4uth.gov.ua/	Державна бібліотека України для юнацтва (Київ)