ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

ЗАТВЕРДЖЕНО
вченою радою
(пост. п. 9 від «30» 06 2022 р.)
Ректор
_____ А. А. Мазаракі

ОСНОВИ КІБЕРБЕЗПЕКИ / CYBERSECURITY ESSENTIALS

РОБОЧА ПРОГРАМА / COURSE OUTLINE

освітній ступінь	**бакалавр**	/	bachelor
галузь знань	**05 Соціальні та поведінкові науки**	/	Social and behavioral sciences
спеціальність	**053 Психологія**	/	Psychology
освітня програма	**Практична психологія**	/	Practical psychology

Київ 2022

Автори: Ю.В. КОСТЮК, старший викладач кафедри інженерії програмного забезпечення та кібербезпеки,
Т.В. САВЧЕНКО кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Л.О. ВЛАСЕНКО, кандидат технічних наук, доцент, кафедри інженерії програмного забезпечення та кібербезпеки

Робочу програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «14» травня 2022р., протокол №38.

Рецензенти: Н.О. Котенко, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
В.П. Звєрєв, кандидат технічних наук, заступник керівника служби з питань інформаційної безпеки та кібербезпеки – керівник управління інформаційної безпеки Апарату Ради Національної безпеки і оборони України,
І.М. Овдієнко, кандидат психологічних наук, доцент кафедри психології

ОСНОВИ КІБЕРБЕЗПЕКИ /
CYBERSECURITY ESSENTIALS

РОБОЧА ПРОГРАМА /
COURSE OUTLINE

освітній ступінь	**бакалавр**	/	bachelor
галузь знань	**05 Соціальні та поведінкові науки**	/	Social and behavioral sciences
спеціальність	**053 Психологія**	/	Psychology
освітня програма	**Практична психологія**	/	Practical psychology

1. СТРУКТУРА ДИСЦИПЛІНИ «ОСНОВИ КІБЕРБЕЗПЕКИ» ТА РОЗПОДІЛ ГОДИН ЗА ТЕМАМИ (ТЕМАТИЧНИЙ ПЛАН)

Назва теми	Кількість годин				Форми контролю
	Усього год/кредитів	Лекції	Лабораторні заняття / МК	Самостійна робота студ.	
Тема 1. Кіберпростір і кібербезпека ─ головні ознаки нової інформаційної цивілізації	12	1	1	10	К, ЛР, ПСР
Тема 2. Національна система кібербезпеки України	12	1	1	10	К, ЛР, ПСР
Тема 3. Сутність та основні процедури керування кібербезпекою	12	1	2	10	К, ЛР, ПСР
Тема 4. Кібератаки, загрози та їх властивості. Характеристика сучасних кібератак	13	2		10	К, ЛР, ПСР
Тема 5. Дезінформація як елемент кібератак. Сценарії розвитку та методи протидії	12	2	2	8	К, ЛР, ПСР
Тема 6. Комп'ютерна вірусологія	14	2	2	10	К, ЛР, ПСР
Тема 7. Соціальна інженерія	14	2	2	10	К, ЛР, ПСР
Тема 8. Соціотехнічна безпека: проблемні аспекти	14	2	2	10	К, ЛР, ПСР
Тема 9. Безпека спілкування в кіберпросторі	12	2	2	8	К, ЛР, ПСР
Тема 10. Особливості економічної діяльності суб'єктів господарювання в кіберпросторі	12	2	2	8	К, ЛР, ПСР
Тема 11. Безпека цифрового простору суб'єктів господарювання	12	2	2	8	К, ЛР, ПСР
Тема 12. Безпека Інтернету-речей	13	1	2	10	К, ЛР, ПСР
Тема 13. Системи захисту інформації на проникнення	14	2	2	10	К, ЛР, ПСР
Тема 14. Основні методи забезпечення кібербезпеки суб'єкта господарювання	14	2	2	10	К, Т, ЛР, ПСР, ПК
Разом	180/6	24	24	132	
Підсумковий контроль – екзамен					

Примітка: Т – тестування; ЛР – захист лабораторних робіт; ПСР – перевірка самостійної роботи; ПК - підсумковий контроль; К – конспект.

2. ТЕМАТИКА ТА ЗМІСТ ЛЕКЦІЙНИХ, ЛАБОРАТОРНИХ ЗАНЯТЬ ТА САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
ТЕМА 1. КІБЕРПРОСТІР І КІБЕРБЕЗПЕКА — ГОЛОВНІ ОЗНАКИ НОВОЇ ІНФОРМАЦІЙНОЇ ЦИВІЛІЗАЦІЇ		
Знати: Поняття кібербезпеки, кіберпростору, кібероротьби, кібертероризму, кіберзброї; типові загрози для користувачів, промисловості, способу життя людей; наслідки порушення кібербезпеки ***Вміти:*** Класифікувати зловмисників; ідентифікувати загрози.	**Лекція №1** ***Кіберпростір і кібербезпека — головні ознаки нової інформаційної цивілізації.*** *План лекції №1* 1. Поняття інформаційна безпека, кібербезпека, кіберпростір, кібероротьба, кібертероризм, кіберзброя**.** 2. Кіберпростір: визначення, система відношень, загрози. Потреба в кібербезпеці. 3. Кіберінциденти: передумови скоєння та наслідки. 4. Поняття «кібервійни». Захист даних та конфіденційності в професійній діяльності психолога**.** 5. Огляд областей кібербезпеки. Приклади доменів кібербезпеки. 6. Поняття «кіберзлочинець» та мотиви кіберзлочинів. Класифікація зловмисників**.** **Список рекомендованих джерел:** *Основний: 1[с. 50-59, 66-98, 257-268, 310-312], 2 [с. 7-43], 3 [с. 27-38, 130-146], 4 [с. 112-120].* *Додатковий: 6 [с. 25-28, 172-176, 239, 249-252, 255-263].* *Інтернет-ресурси: 14.*	1

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	Самостійна робота студентів. Вивчення лекційного матеріалу. Опрацювати матеріал: «Наслідки порушення кібербезпеки», поняття «кіберзлочинець» та мотиви кіберзлочинів»; «Класифікація зловмисків та загроз». **Список рекомендованих джерел:** *Основний: 1[с. 50-59, 66-98, 257-268, 310-312], 2 [с. 7-43], 3 [с. 27-38, 130-146], 4 [с. 112-120].* *Додатковий: 6 [с. 25-28, 172-176, 239, 249-252, 255-263].* *Інтернет-ресурси: 14.*	10
	Лабораторне заняття №1 **Кібернетичний простір та доступ до системи WWW за допомогою веб-браузера** **Мета: 1)** поглиблення та закріплення теоретичних знань з наступних питань: - кібернетичний простір: термінологія, структура; - поява та розвиток Інтернет; - основні поняття системи WWW; - структура верхнього рівня веб-браузера. 2) набуття практичних навичок роботи з веб-браузерам **Завдання:** 1) виконати теоретичне завдання згідно з номером варіанту, який приведено в табл. 1, особливо звернути увагу на механізми забезпечення	1

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	інформаційної безпеки в веб-браузера в професійній дяльності психолога. 2) Знайти і обробити інформацію відповідно до завдання та підготувати коротку доповідь (міні-презентацію). 3) провести порівняльний аналіз 2-3 обраних браузерів та сформувати відповідну порівняльну таблицю щодо забезпечення інформаційної безпеки. 4). Оформити звіт згідно до вимог (додаток 1). 5). Зробити висновки, відповісти письмово на контрольні питання та підготуватися до усного опитування.	
ТЕМА 2. НАЦІОНАЛЬНА СИСТЕМА КІБЕРБЕЗПЕКИ УКРАЇНИ		
Знати: розуміти окремі аспекти вітчизняного законодавства, яке має давні традиції унормування правил безпечної роботи з інформацією; структуру національної безпеки України; основні пріоритети забезпечення інформаційної безпеки;.	**Лекція №2** ***Національна система кібербезпеки України*** *План лекції №2* 1. Національна безпека України: реалії та перспективи. Роль та місце кібернетичної безпеки у загальній системі нацбезпеки. 2. Основні положення Стратегії кібербезпеки України. 3. Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці. 4. Правове забезпечення у сфері інформаційної безпеки та кібербезпеки. **Список рекомендованих джерел:** *Основний: 1 [с. 135-149], 2 [с. 7-24], 3 [с. 222-240], 4 [с. 137-138].* *Додатковий: 6 [с. 189-209], 7 [с. 93-106], 10, 11, 12.* *Інтернет-ресурси: 14, 16.*	1

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
Вміти: Класифікувати інформацію за порядком доступу на відкриту та з обмеженим доступом		
	Самостійна робота студентів. Вивчення лекційного матеріалу; опрацювати матеріал: «Суб'єкти забезпечення інформаційної безпеки як складової національної безпеки України»; організаційна структура охорони державної таємниці. **Список рекомендованих джерел:** *Основний: 1 [с. 135-149], 2 [с. 7-24], 3 [с. 222-240], 4 [с. 137-138].* *Додатковий: 6 [с. 189-209], 7 [с. 93-106], 10, 11, 12.* *Інтернет-ресурси: 14, 16.*	10
	Лабораторне заняття №2 **Інформаційна безпека держави. Потенційні загрози, засоби їх попередження та ліквідації** **Мета:** ознайомитися з поняттям інформаційної безпеки держави та інформаційної війни, основними інтересами України та потенційними небезпеками у сфері інформаційної безпеки, елементами інформаційної боротьби; законодавством України, що стосується інформаційної безпеки держави. **Завдання:** 1) Користуючись однією з пошуковх систем (Google, чи будь-якою іншою) ознайомтеся із законодавчою базою України, що стосується інформаційної безпеки держави. Назви основних законів, указів президента, постанов, положень записати до звіту (не менше 10). 2) На офіційному сайті Верховної ради «Законодавство України» (http://zakon2.rada.gov.ua/laws) знайдіть Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015	1

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	роки», ознайомтесь з його основними положеннями та занотуйте до звіту такі відомості: - основні стратегічні цілі розвитку інформаційного суспільства в Україні; - основні напрямки розвитку інформаційного суспільства в Україні; - законодавче забезпечення розвитку інформаційного суспільства; - інформаційна безпека в інформаційному суспільстві. 3) Користуючись однією з пошукових систем (Google, чи будь-якою іншою) знайдіть текст Доктрини інформаційної безпеки України, ознайомтесь з основними положеннями та занотуйте до звіту такі відомості: - основні напрями забезпечення державою національного інформаційного суверенітету; - принципи забезпечення інформаційної безпеки України; - основні реальні та потенційні загрози інформаційній безпеці України у сфері державної безпеки; - основні засади державної політики забезпечення інформаційної безпеки України; зробити висновки та письмово дати відповіді на питання.	
ТЕМА 3. СУТНІСТЬ ТА ОСНОВНІ ПРОЦЕДУРИ КЕРУВАННЯ КІБЕРБЕЗПЕКОЮ		
Знати: три виміри куба кібербезпеки; принципи конфіденційності; принцип доступності; модель кібербезпеки ISO; типи сховищ даних, методи передачі даних; проблеми що	**Лекція №3** ***Сутність та основні процедури керування кібербезпекою*** *План лекції №3* 1. Модель кібербезпеки ISO. 2. Куб кібербезпеки. 2. Захист конфіденційності даних в професійній діяльності психолога. Керування доступом. 3. Потреба в цілісності даних. Перевірка цілісності в професійній діяльності	1

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
пов’язані із захистом збережених даних; проблеми захисту даних у процесі обробки. ***Вміти:*** захистити конфіденційні дані; шифрувати файли і дані.	психолога. 4. Принцип доступності. П'ять дев'яток. Забезпечення доступності. 5. Проблеми захисту збережених даних. Методи передачі даних. Проблеми захисту даних у процесі обробці в професійній діяльності. ***Список рекомендованих джерел:*** *Основний: 1 [с. 54-59], 3 [с. 157-166].* *Додатковий: 6 [с. 218-219].* *Інтернет-ресурси: 14, 15, 16.* **Самостійна робота студентів**. Вивчення лекційного матеріалу; опрацювати матеріал: проблеми захисту даних під час передачі, проблеми захисту даних у процесі обробці, модель кібербезпеки ISO; куб кібербезпеки; принципи конфіденційності; принцип доступності. **Список рекомендованих джерел:** *Основний: 1 [с. 54-59], 3 [с. 157-166].* *Додатковий: 6 [с. 218-219].* *Інтернет-ресурси: 14, 15, 16.*	10
ТЕМА 4. КІБЕРАТАКИ, ЗАГРОЗИ ТА ЇХ ВЛАСТИВОСТІ. ХАРАКТЕРИСТИКА СУЧАСНИХ КІБЕРАТАК		
Знати: Класифікація кібератак; аналіз трафіку (Sniffing);	**Лекція №4** ***Кібератаки, загрози та їх властивості. Характеристика сучасних кібератак*** *План лекції №4* 1. Сутність та класифікація кібератак. Етапи реалізації атак.	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
атаки нульового дня; клавіатурні шпигуни Grayware та SMiShing; несанкціоновані точки доступу; глушіння радіочастот (RF Jamming); Bluejacking та Bluesnarfing; атаки на WEP та WPA; міжсайтовий скриптинг; ін'єкція коду; розподілена DoS атака (Distributed DoS Attack, DDoS); отруєння SEO ***Вміти:*** Захист від атак на бездротові мережі та мобільні пристрої, застосунки	2. Атаки на бездротові мережі та мобільні пристрої. Атаки на WEP та WPA. 3. Атаки на застосунки. Міжсайтовий скриптинг. Ін'єкція коду. Переповнення буфера. Віддалений запуск програм. 4. Атака "Відмова в обслуговуванні" (DoS). Розподілена DoS атака (Distributed DoS Attack, DDoS). 5. Зміст, класифікація та ознаки кіберзагроз. Основні характеристики кіберзагроз. Поширення кіберзагроз. Кіберзагрози підвищеної складності. **Список рекомендованих джерел:** *Основний: 1 [с. 66-96, 168-179], 2 [с. 43-62], 3 [с. 92-138], 4 [с. 9-23].* *Додатковий: 6 [с. 296-299, 340-354], 8 [с. 50-82, 197-201].* *Інтернет-ресурси: 14, 15.*	
	Самостійна робота студентів. Вивчення лекційного матеріалу; опрацювати матеріал: «Кіберзагрози через Інтернет-сервіси. Поширення кіберзагроз. Кіберзагрози підвищеної складності. Проаналізувати: атака "Відмова в обслуговуванні" (DoS); розподілена DoS атака (Distributed DoS Attack, DDoS); отруєння SEO**.** **Список рекомендованих джерел:** *Основний: 1 [с. 66-96, 168-179], 2 [с. 43-62], 3 [с. 92-138], 4 [с. 9-23].* *Додатковий: 6 [с. 296-299, 340-354], 8 [с. 50-82, 197-201].* *Інтернет-ресурси: 14, 15.*	10
	Лабораторне заняття №3	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	Візуалізація «чорних» хакерів ***Ідентифікація загроз*** **Мета: 1)** Вивчення та аналіз інцидентів кібербезпеки. 2) Вивчення можливостей забезпечення функцій безпеки, які використовуються організаціями для збереження даних. **Завдання: 1)** після дослідження та аналізу дати відповіді на запитання: Хто є хакером? До якої організації або групи належить хакер? Який мотив у хакера? Який метод атаки був використаний? Що було метою і в чому була вразливість, використана проти компанії? Як можна було запобігти цій атаці або зменшити її наслідки? 2) Дослідити загрози, що витікають від кібератак. Дослідити тріаду CIA (конфіденційність, цілісність і доступність) та типи кібератак.	
ТЕМА 5. ДЕЗІНФОРМАЦІЯ ЯК ЕЛЕМЕНТ КІБЕРАТАК. СЦЕНАРІЇ РОЗВИТКУ ТА МЕТОДИ ПРОТИДІЇ		
Знати: Поняття «дезінформації»; типи неправдивої інформації; виявлення неправдивих повідомлень; види маніпуляцій	**Лекція №5** ***Дезінформація як елемент кібератак. Сценарії розвитку та методи протидії*** *План лекції №5* 1. Канали поширення дезінформації. Типи неправдивої інформації в професійній діяльності. 2. Технології неправдивих повідомлень. Інструменти виявлення неправдивих повідомлень. 3. Види маніпуляцій. Пропаганда як інструментів інформаційного впливу в	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
маніпуляції з медіаданими, **Вміти:** Виявлення неправдивих повідомлень; протидії неправдивим повідомленням.	професійній діяльності. 4.Маніпулювання новинами. Маніпулювання експертними оцінками. Маніпулювання повідомленнями. Маніпуляції з результатами досліджень. **Список рекомендованих джерел:** *Основний: 3 [с. 19, 43-60, 64-79], 4 [с. 97-102].* *Додатковий: 7 [с. 87-90].* *Інтернет-ресурси: 14, 15.*	
	Самостійна робота студентів. Вивчення лекційного матеріалу; опрацювати матеріал: види маніпуляцій: маніпуляції новинами; маніпуляції експертними оцінками; маніпуляції повідомленнями; маніпуляції результатами досліджень **Список рекомендованих джерел:** *Основний: 3 [с. 19, 43-60, 64-79], 4 [с. 97-102].* *Додатковий: 7 [с. 87-90].* *Інтернет-ресурси: 14, 15.*	8
	Лабораторне заняття №4 **Підвищення безпеки облікового запису Google** **Мета:** Захист особистих даних в професійній діяльності. Підвищення безпеки облікового запису Google. Краще зрозуміти заходи безпеки та сервіси, які такі організації, як Google, здійснюють для захисту інформації в професійній діяльності та інформаційних систем .	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	Завдання: 1) Проаналізувати можливості функцій безпеки, які використовують такі організації, як Google та Cisco, для захисту даних. Дізнатися як Google гарантує, що сервери, які вони встановлюють у своїх центрах обробки даних (ЦОД), не заражені зловмисним програмним забезпеченням виробниками обладнання. 2) Визначення вразливостей даних. 3) Вміти захистити доступ до облікового запису Gmail.	
ТЕМА 6. КОМП'ЮТЕРНА ВІРУСОЛОГІЯ		
Знати: Поняття «комп'ютерні віруси»; класифікація комп'ютерних вірусів**;** типи шкідливого програмного забезпечення (ШПЗ); шляхи розповсюдження та симптоми зараження ШПЗ; завантажувач (дропер/лоадер); викрадач інформації	**Лекція №6** ***Комп'ютерна вірусологія*** *План лекції №6* 1. Поняття про комп'ютерні віруси, історія їх виникнення та розвитку. Загальні принципи функціонування комп'ютерних вірусів, їх розмноження. Алгоритми роботи вірусів. 2. Класифікація комп'ютерних вірусів: файлові, завантажувальні (бутові) та файлово-завантажувальні віруси, макровіруси, мережні віруси. 3. Класифікаційний код вірусу. Резидентність, використання стелсалгоритмів, самошифрування та поліморфізм, використання нестандартних методів. 4. Шкідливе програмне забезпечення (ШПЗ). Шляхи розповсюдження ШПЗ, вектори атак. Типи шкідливого програмного забезпечення. Симптоми зараження шкідливим ШПЗ. Шпигунські програми (spyware). 5. Завантажувач (дропер/лоадер). Викрадач інформації «інфостілер або стілер». Keylogger "кейлогер". «JS-сніфери». Троянські програми віддаленого доступу.rat. Банківські трояни (banking trojans). Ransomware (програма-вимагач, програма-	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
«інфостілер або стілер»; Keylogger “кейлогер”; «JS-сніфери»; троянські програми віддаленого доступу .rat; банківські трояни (banking trojans); Ransomware (програма-вимагач, програма-шантажист); майнери (miners) ***Вміти*:** виявляти загрози та вразливості	шантажист). Майнери (miners). 6. Шкідливе програмне забезпечення для знищення інформації без можливості її відновлення. 7. Рекламне шкідливе програмне забезпечення (adware). **Список рекомендованих джерел:** *Основний: 3 [с. 170-211].* *Додатковий: 7 [с. 69-96].* *Інтернет-ресурси: 14, 15*	
	Самостійна робота студентів. Вивчення лекційного матеріалу. Ознайомитись із інформацією про клавіатурних шпигунів (кейлогерів); класифікація комп’ютерних вірусів; алгоритми роботи вірусів; типи шкідливого програмного забезпечення (ШПЗ. Опрацювати питання що стосується розповсюдження та симптомів зараження рекламним шкідливим програмним забезпеченням (adware) **Список рекомендованих джерел:** *Основний: 3 [с. 170-211].* *Додатковий: 7 [с. 69-96].* *Інтернет-ресурси: 14, 15.*	10
	Лабораторне заняття №5 **Комп’ютерні віруси: знайомство з принципами роботи. Захист від вірусів в професійній діяльності. Огляд основних антивірусних програм** **Мета:** ознайомитись з основними видами комп’ютерних вірусів, принципами їх роботи поширення і знищення. Розглянути програми для захисту від вірусів, принцип дії, ефективність, можливості.	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	Завдання: вибрати один з типів вірусів і описати його за планом: назви вірусів даного типу; принцип роботи даного типу вірусів; методи поширення даного типу вірусів; програми для знищення даного типу вірусів; методи для знищення даного типу вірусів. Оформити звіт по роботі та дати письмово відповідь на контрольні питання.	
ТЕМА 7. СОЦІАЛЬНА ІНЖЕНЕРІЯ		
Знати: Методи соціальної інженерії; види атак соціальної інженерії; тактики соціальної інженерії; фішингова атака; етапи атаки із використанням СІ; розвідка та збір інформації; використання вразливостей як розповсюджений метод проникнення для отримання інформації ***Вміти:*** виявляти	**Лекція №7** ***Соціальна інженерія*** *План лекції №7* 1. Поняття соціальної інженерії. Методи соціальної інженерії. 2. Види атак соціальної інженерії. Претекстінг (pretexting). Тейлгейтінг (tailgating). Послуга за послугу (quid pro quo). Злам пароля WI-FI. Атаки грубої сили (brute-force attacks). Прослуховування мережі (network sniffing). 3. Фішингова атака. 4. Етапи атаки із використанням СІ **(**соціальної інженерії). Легендування та планування атаки із використання методів СІ. 5. Використання вразливостей як розповсюджений метод проникнення для отримання інформації в професійній діяльності психолога **Список рекомендованих джерел:** *Основний: 2 [с. 112-148], 3 [с. 83-91].* *Додатковий: 6 [с. 136-140], 7 [с. 8-25].* *Інтернет-ресурси: 14.*	2
	Самостійна робота студентів. Вивчення лекційного матеріалу; опрацювати матеріал: «Тактики соціальної інженерії», «Розвідка та збір інформації із	10

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
загрози та вразливості	відкритих джерел». **Список рекомендованих джерел:** *Основний: 2 [с. 112-148], 3 [с. 83-91].* *Додатковий: 6 [с. 136-140], 7 [с. 8-25].* *Інтернет-ресурси: 14*	
	Лабораторне заняття №6 **Хто володіє даними: правила надання послуг** **Мета:** Дослідити яким є право власності на особисті дані, якщо вони зберігаються не в локальній системі. Ознайомитися з правилами надання послуг. **Завдання:** дослідити правові угоди, необхідні для використання різних онлайн-сервісів. Дізнатися про деякі способи захисту особистих даних.	2
ТЕМА 8. СОЦІОТЕХНІЧНА БЕЗПЕКА: ПРОБЛЕМНІ АСПЕКТИ		
Знати: Основні аспекти, поняття та визначення соціальної інженерії як методи розвідки складних соціальних і соціотехнічних систем; поняття соціотехнічної системи та її властивостей;	**Лекція №8** ***Соціотехнічна безпека: проблемні аспекти*** *План лекції №8* 1. Соціальна інженерія як метод розвідки складних соціальних і соціотехнічних систем в професійній діяльності психолога. 2. Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу. 3. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки. 4. Соціальні мережі: особливості, основні поняття та визначення. Моніторинг соціальних мереж − цілі та способи реалізації. 5. Поняття соціотехнічної системи та її властивостей. 6. Системний підхід як загальнометодологічний принцип створення складних	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
соціальні мережі: особливості, основні поняття та визначення; моніторинг соціальних мереж − цілі та способи реалізації. ***Вміти:*** захист сучасної інфосфери в умовах стороннього кібернетичного впливу;	соціотехнічних систем. **Список рекомендованих джерел:** *Основний: 2 [с. 64-95].* *Додатковий: 6 [с. 144-159], 7 [с. 97-99].* *Інтернет-ресурси: 14*	
	Самостійна робота студентів. Вивчення лекційного матеріалу; опрацювати матеріал: «Поняття соціотехнічної системи та її властивостей»; «Методи забезпечення інформаційної і кібербезпеки»; «Соціальні мережі: особливості, основні поняття та визначення». **Список рекомендованих джерел:** *Основний: 2 [с. 64-95].* *Додатковий: 6 [с. 144-159], 7 [с. 97-99].* *Інтернет-ресурси: 14*	10
	Лабораторне заняття №7 **Інциденти порушення безпеки, несанкціонований доступ до даних** **Мета:** Знайти інформацію та прочитати про деякі нещодавні порушення безпеки; ознайомитись з декількома інцидентами порушення безпеки, щоб визначити, що було зроблено, які експлойти було використано, і що потрібно зробити, щоб захистити особисті дані в професійній діяльності психолога. **Завдання:** Використовуючи три надані посилання, в яких описано порушення безпеки у різних секторах, заповнити таблицю. Знайти декілька додаткових цікавих випадків порушень кібербезпеки та зазначити їх у висновку в таблиці	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
ТЕМА 9. БЕЗПЕКА СПІЛКУВАННЯ В КІБЕРПРОСТОРІ		
Знати: Характер проведення атак у глобальних мережах; захист інформації в глобальних мережах; безпечне користування мережею «Інтернет»; найпоширеніші способи нелегального заробітку в мережі «Інтернет»; безпека браузерів; безпека даних. ***Вміти:*** Захист під час використання WWW (World Wide Web); безпечне користування месенджерами; безпечне	**Лекція №9** ***Безпека спілкування в кіберпросторі в професійній діяльності психолога*** *План лекції №9* 1. Захист інформації в глобальних мережах. 2. Характер проведення атак у глобальних мережах. 3. Безпечне користування мережею «Інтернет». 4. Найпоширеніші способи нелегального заробітку в мережі «Інтернет». 5. Безпека браузерів. 6. Безпека даних в діяльності психолога. 7. Безпечне користування мережами WI-FI. Основні правила безпечного користування WI-FI в діяльності психолога. 8. Безпечне користування месенджерами в професійній діяльності. **Список рекомендованих джерел:** *Основний: 2 [с. 24-43].* *Додатковий: 6 [с. 495-508], 7 [с. 41-52].* *Інтернет-ресурси: 14*	2
	Самостійна робота студентів. Вивчення лекційного матеріалу; опрацювати матеріал: «Безпечне користування мережею «Інтернет»; «Безпека браузерів»;	8

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
користування мережами WI-FI.	«Безпека даних», «Безпечне користування месенджерами»; «Безпечне користування мережами WI-FI». **Список рекомендованих джерел:** *Основний: 2 [с. 24-43].* *Додатковий: 6 [с. 495-508], 7 [с. 41-52].* *Інтернет-ресурси: 14*	
	Лабораторне заняття №8 **Захист комп'ютерних мереж та персональних комп'ютерів за допомогою брандмауера (Firewall)** **Мета:** ознайомитися з основним типами, призначенням, базовими функціями брандмауера, зробити загальний огляд вбудованого брандмауера операційної системи Windows. **Завдання:** 1) Виконати послідовність дій Пуск, Панель управления, Система и безопасность, Братмауэр Windows. 2) З'ясувати стан підключення брандмауера. Якщо він відключений – включіть його. Налаштування брандмауера Windows відбувається, в першу чергу, шляхом вказівки "Винятків". 3) Створити виняток для програми, яка повинна приймати вихідні підключення з мережі. Щоб створити виняток потрібно натиснути кнопку "Додати програму ...."	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	відкриється вікно, приклад якого показаний нижче. У цьому вікні в списку програм перераховані ті з них, які встановлені на комп'ютері. Якщо програма, якою необхідно дозволити приймати вхідні підключення, відсутній у списку, то за допомогою кнопки Огляд можна вказати шлях до неї. Після натискання кнопки ОК виключення буде створено і додано до списку, де буде зазначено прапорцем, який говорить про те, що дане правило дозволяє зазначеним Додатком відкривати порти і чекати підключення з мережі. Якщо необхідно заборонити додатком відкривати порти, то прапорець слід зняти. 4) Письмово дати відповідь на питання.	
ТЕМА 10. ОСОБЛИВОСТІ ЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ В КІБЕРПРОСТОРІ		

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
Знати: Безпека користування соціальними мережами; головні правила роботи з мобільними пристроями оновлення паролів та парольних фраз; конфіденційність даних; налаштування конфіденційності та інших питань безпеки; найвідоміші атаки через електронну пошту; безпека мобільних пристроїв; блокування доступу до пристрою; загрози під час користування поштовою скринькою; легітимні та фішингові листи	**Лекція №10** ***Особливості економічної діяльності суб'єктів господарювання в кіберпросторі*** *План лекції №10* 1. Безпека користування соціальними мережами в професійній діяльності психолога. Реєстрація. Стійкий пароль. Оновлення паролів та парольних фраз. 2. Конфіденційність даних. Налаштування конфіденційності та інших питань безпеки в професійній діяльності психолога. 3. Безпека мобільних пристроїв. Блокування доступу до пристрою. Безпечна робота в мультимедійних засобах спілкування в професійній діяльності психолога. Передавання вживаних мобільних пристроїв іншим особам. Передавання контактної інформації іншим особам. Вірусне програмне забезпечення. Додаткові функції мобільного пристрою. Головні правила роботи з мобільними пристроями. 4. Безпека користування електронною поштою в професійній діяльності психолога. Конфіденційність електронної пошти. Найвідоміші атаки через електронну пошту. Загрози під час користування поштовою скринькою. Легітимні та фішингові листи (investigation). 5. Забезпечення безпеки особистої поштової скриньки (рекомендації). **Список рекомендованих джерел:** *Основний: 2 [с. 130-147], 4[с. 35-49, 68-70].* *Додатковий: 7 [с. 55-67, 97-99, 105-123].* *Інтернет-ресурси: 14*	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
(investigation). ***Вміти:*** безпека мобільних пристроїв; блокування доступу до пристрою; безпечна робота в мультимедійних засобах спілкування; забезпечення безпеки особистої поштової скриньки	**Самостійна робота студентів**. Вивчення лекційного матеріалу; опрацювати матеріал: «Стійкий пароль. Оновлення паролів та парольних фраз». Безпека користування соціальними мережами; головні правила роботи з мобільними пристроями; безпека мобільних пристроїв; блокування доступу до пристрою; безпечна робота в мультимедійних засобах спілкування; забезпечення безпеки особистої поштової скриньки **Список рекомендованих джерел:** *Основний: 2 [с. 130-147], 4[с. 35-49, 68-70].* *Додатковий: 7 [с. 55-67, 97-99, 105-123].* *Інтернет-ресурси: 14*	8
	Лабораторне заняття №9 ***Створення та збереження надійних паролів*** **Мета:** Один із найважливіших способів захистити свої облікові записи в Інтернеті – захистити паролі**.** Зрозуміти концепцію надійного пароля. Необхідно мати різні паролі для різних служб. Часте оновлення паролів є обов'язковим. Рекомендується використання (не дуже розумних або ж навпаки улюблених) фраз як спосіб створення паролів. Потрібно завжди пам’ятати про використання двоетапної перевірки вашого пароля. **Завдання:** Дослідження концепцій створення надійного пароля: створення надійного пароля. Дослідження концепцій безпечного збереження паролів: безпечне зберігання паролів. Використовуючи характеристики надійного пароля,	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	вибрати пароль, який легко запам'ятати, але важко вгадати. Використати для зберігання паролей менеджер паролів.	
ТЕМА 11. БЕЗПЕКА ЦИФРОВОГО ПРОСТОРУ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ		
Знати: Класифікація каналів витоку інформації; методи та засоби блокування технічних каналів витоку інформації; захист акустичної інформації від зняття радіопристроями; захист інформації від несанкціонованого запису звукозаписувальними пристроями; захист електронної інформації; захист письмової інформації від оптичного зняття. ***Вміти:***	**Лекція №11** ***Безпека цифрового простору суб'єктів господарювання*** *План лекції №11* 1. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів її витоку. 2. Класифікація каналів витоку інформації. Методи блокування технічних каналів витоку інформації. 3. Системи та засоби виявлення, пошуку та знешкоджування технічних засобів зняття інформації. 4. Захист акустичної інформації від зняття радіопристроями. 5. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами. 6. Захист інформації від несанкціонованого запису звукозаписувальними пристроями. 7. Захист електронної інформації в професійній діяльності психолога. 8. Захист письмової інформації від оптичного зняття в професійній діяльності. **Список рекомендованих джерел:** *Основний: 2 [с. 151-181], 3 [с. 43-60, 290-305].* *Додатковий: 7 [с. 123-127].* *Інтернет-ресурси: 14*	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
проводити аналіз, виявляти та знешкоджування технічні засоби зняття інформації		
	Самостійна робота студентів. Вивчення лекційного матеріалу; опрацювати матеріал: «Засоби блокування технічних каналів витоку інформації» **Список рекомендованих джерел:** *Основний: 2 [с. 151-181], 3 [с. 43-60, 290-305].* *Додатковий: 7 [с. 123-127].* *Інтернет-ресурси: 14*	8
	Лабораторне заняття №10 ***Перевірка факту компрометації поштової адреси.*** ***Двофакторна автентифікація поштового облікового запису*** **Мета:** 1) пересвідчитись у відсутності або наявності витоку власних автентифікаційних даних; 2) відпрацювати навички налаштування двофакторної автентифікації для різних облікових записів. **Завдання:** 1) за адресами https://haveibeenpwned.com , https://monitor.firefox.com перевірити наявність власних поштових облікових записів у «зливах», де фігурують вкрадені дані автентифікації. у випадку знаходження поштових облікових записів у «зливах» терміново змінити паролі на відповідних ресурсах та, за можливості, налаштувати двофакторну автентифікацію; 2) створити безкоштовні особисті поштові облікові записи в доменах gmail.com та protonmail.com. Налаштувати двофакторну автентифікацію через Google Authenticator для облікових записів gmail.com та protonmail.com.	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
ТЕМА 12. БЕЗПЕКА ІНТЕРНЕТУ-РЕЧЕЙ		
Знати: Архітектура Інтернету-речей; технології Інтернету-речей; анатомія кібератак на IoT-пристрої; симетрична і асиметрична криптографія; аутентифікація і цифровий підпис; блокчейн і криптовалюта в Інтернеті-речей ***Вміти:*** Захист IoT-пристроїв	**Лекція №12** ***Безпека Інтернету-речей*** *План лекції №12* 1. Історія Інтернету-речей. Екосистема Інтернету-речей. 2. Архітектура Інтернету-речей. Технології Інтернету-речей. «Розумний та безпечний будинок». 3. Анатомія кібератак на IoT-пристрої. Mirai. Stuxnet. Ланцюжкова реакція. Туманні технології. 4. Криптографія. Симетрична криптографія. Асиметрична криптографія. 5. Криптографічний хеш (аутентифікація і цифровий підпис). 6. Інфраструктура відкритого ключа. 7. Блокчейн і криптовалюта в Інтернеті-речей. 8. Рекомендації щодо захисту IoT-пристроїв в професійній діяльності психолога. **Список рекомендованих джерел:** *Основний: 2 [с. 163-167].* *Додатковий: 6 [с. 398-404, 480-482], 9 [с. 15-18, 111-127, 159-170, 189-200].* *Інтернет-ресурси: 14*	1
	Самостійна робота студентів. Вивчення лекційного матеріалу; опрацювати матеріал: «Кібератаки на IoT-пристрої. Mirai. Stuxnet. Ланцюжкова реакція». **Список рекомендованих джерел:** *Основний: 2 [с. 163-167].* *Додатковий: 6 [с. 398-404, 480-482], 9 [с. 15-18, 111-127, 159-170, 189-200].*	10

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	Інтернет-ресурси: 14	
	Лабораторне заняття №11 ***Використання цифрових підписів*** **Мета:** зрозуміти концепції цифрового підпису**,** оскільки мета цифрового підпису полягає в тому, щоб запобігти підробці та інперсоніфікації цифрових повідомлень **Завдання:** продемонструвати використання цифрових підписів (використовувати веб-сайт для перевірки підпису документа); продемонструвати перевірку цифрового підпису; створення власного цифрового підпису.	2
ТЕМА 13. СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПРОНИКНЕННЯ		
Знати: Апаратні засоби, мережні технології та хмарні технології захисту; атака через фізичне втручання: Stuxnet; методи та моделі стеганографії; комп'ютерна і цифрова стеганографія, цифрові водяні позначки. Практичні	**Лекція №13** ***Системи захисту інформації на проникнення в професійній діяльності психолога*** *План лекції №13* 1. Технології захисту на основі програмного забезпечення. Апаратні засоби захисту. Мережні технології захисту. Хмарні технології захисту в професійній діяльності психолога. 2. Фізична безпека. Загрози, пов’язані з недотриманням правил фізичної безпеки. Найпопулярніша атака через фізичне втручання: Stuxnet. 3. Захист інформації за допомогою міжмережних екранів (брандмауера). 4. Маскування даних. Технології маскування даних. Стеганографія, основні терміни та визначення. Методи та моделі стеганографії. Комп'ютерна і цифрова стеганографія, цифрові водяні позначки.	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
аспекти побудови стеганосистем ***Вміти:*** Виявляти загрози, пов’язані з недотриманням правил фізичної безпеки; захист інформації за допомогою міжмережних екранів	5. Практичні аспекти побудови стеганосистем в професійній діяльності психолога. Приховування даних у текстових файлах: методи текстової стеганографії; аналіз реалізації методів. **Список рекомендованих джерел:** *Основний: 1 [с. 188-205], 2 [с. 158-159], 3 [с. 290-312].* *Додатковий: 7 [с. 123-127].* *Інтернет-ресурси: 14*	
	Самостійна робота студентів. Вивчення лекційного матеріалу; опрацювати матеріал: «Історичні приклади стеганосистем. Галузі застосування стеганографії», «методи та моделі стеганографії; комп'ютерна і цифрова стеганографія»; «Технології маскування даних», Апаратні засоби, мережні технології та хмарні технології захисту. **Список рекомендованих джерел:** *Основний: 1 [с. 188-205], 2 [с. 158-159], 3 [с. 290-312].* *Додатковий: 7 [с. 123-127].* *Інтернет-ресурси: 14*	10
	Лабораторне заняття №12 **Резервне копіювання даних користувача до зовнішнього сховища** **Мета:** 1) Використання локального зовнішнього диску для резервного копіювання даних; 2) Використання віддаленого диску для резервного копіювання даних. **Завдання:** Дослідити переваги резервного копіювання даних на локальний зовнішній диск. Робота фокусується на Microsoft Backup Utility для виконання	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	резервних копій на локальні зовнішні диски. У другій частині лабораторної роботи використати службу Dropbox для резервного копіювання даних на віддалений або хмарний диск.	
ТЕМА 14. ОСНОВНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СУБ'ЄКТА ГОСПОДАРЮВАННЯ		
Знати: Контроль фізичного доступу; системи розмежування логічного доступу; адміністративний контроль доступу; поняття: криптографії; шифрування за ключами; ідентифікації; аутентифікації; авторизації; стеганографії; соціальної стеганографії; обфускації даних; типи криптографії та типи	**Лекція №14** ***Основні методи забезпечення кібербезпеки суб'єкта господарювання*** *План лекції №14* 1. Типи контролю доступу в професійній діяльності психолога. 2. Стратегії контролю доступу. Дискреційне розмежування доступу. Контроль доступу на основі ролей. Розмежування доступу на основі правил. 3. Ідентифікація. Методи аутентифікації. Багатофакторна аутентифікація. Аутентифікація на основі одноразових паролей. Строга аутентифікація. Криптографічні протоколи строгої аутентифікації. Біометрична аутентифікація користувача. Використання авторизації. 4. Типи засобів контролю безпеки. Превентивні засоби контролю. Стримуючі засоби контролю. Коригуючі засоби контролю. Засоби відновлення. Компенсуючі засоби контролю. 5. Криптографія і її основні поняття. Модель криптографічної системи. Принцип Керкхоффса. Етапи розвитку криптографічних систем. Види історичних шифрів. 6. Типи шифрування. Шифрування за допомогою закритого ключа. Процес симетричного шифрування. Типи криптографічних перетворень. Симетричні криптосистеми шифрування. Алгоритм шифрування DES, 3-DES. Стандарт шифрування AES. Основні режими роботи блочного симетричного алгоритму.	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
криптографічних перетворень; типи контролю доступу; **Вміти:** використовувати засоби відновлення; створювати повідомлення використовуючи шифрування та його дешифрування; використовувати стеганографію.	**Список рекомендованих джерел:** *Основний: 1 [с. 188-193, 205-210], 3 [с. 318-348].* *Додатковий: 6 [с. 398-411, 480-491].* *Інтернет-ресурси: 14*	
	Самостійна робота студентів. Вивчення лекційного матеріалу; Ознайомитись поглиблено «Типи шифрування. Шифрування за допомогою закритого ключа. Процес симетричного шифрування. Типи криптографічних перетворень». Опрацювати теми: «Поняття криптографії та типи криптографічних перетворень» **Список рекомендованих джерел:** *Основний: 1 [с. 188-193, 205-210], 3 [с. 318-348].* *Додатковий: 6 [с. 398-411, 480-491].* *Інтернет-ресурси: 14*	10
	Лабораторне заняття №13 ***Криптографічний вид захисту інформації. Поняття шифрування файлів, папок, повідомлень. Засоби здійснення шифрування інформації в професійній діяльності психолога.*** **Мета:** ознайомитися з поняттям криптографії, способами шифрування файлів, папок, повідомлень та криптографічними методами захисту інформації, розглянути основні засоби здійснення криптографічного захисту інформації; засвоїти принципи, технологію роботи шифрування та дешифрування файлів в	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	професійній діяльності психолога. **Завдання:** 1) Шифр Цезаря — симетричний алгоритм шифрування підстановками. Використовувався римським імператором Юлієм Цезарем для приватного листування. Принцип дії полягає в тому, щоб циклічно зсунути алфавіт, а ключ — це кількість літер, на які робиться зсув. Користуючись алфавітом АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ та використовуючи в якості ключа власний номер в журналі (номер по порядку) зашифрувати повідомлення та записати даний шифр в звіт. «Шифр Цезаря має замало ключів — на одиницю менше, ніж літер в абетці. Тому перебрати усі ключі не складає особливої роботи. Дешифрування з одним з ключів дасть нам вірний відкритий текст». 2) Створення і шифрування повідомлення за допомогою інтерактивних методів. У сучасних мережах використовують багато алгоритмів шифрування різних типів. Одним із найбільш безпечних є симетричний алгоритм блокового шифрування (AES). Використовуватимемо засіб, який можна отримати за наступним посиланням: http://aesencryption.net/. Тому будемо використовувати цей алгоритм у роботі для шифрування та дешифрування.	
Всього		180

***Курсивом виділено теми лекційних та лабораторних занять, які розглядаються із застосуванням інтерактивних методів навчання*

3. *СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ*

Основний

1. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с. ISBN 978-617-582-069-8

2. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.− К.: ДУТ, 2015.− 288 с.

3. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.

4. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

Додатковий

5. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.

6. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с. ISBN 978-617-7844-54-8.

7. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікатної) програми підвищення кваліфікації: Практикум. – Київ: ВАІТЕ, 2021. – 106 с.

8. Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Грищука. – Житомир: ЖНАЕУ, 2019. – 280 с.

9. Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.

10. Указ Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року "Про Стратегію кібербезпеки України" (дата звернення: 30.06.2022).

11. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради України, 2017. – № 45. – Ст.403 (дата звернення: 30.06.2022).

12. Закон України «Про оборону України» // Відомості Верховної Ради України. – 2017. – № 45. – Ст.403 (дата звернення: 30.06.2022).

13. Основи інформаційної безпеки: навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

Інтернет-джерела

14. Cisco -Україна. URL: https://www.cisco.com (дата звернення: 30.06.2022).

15. Annual Threat Reports. URL: https://www.fireeye.com/current-threats/annual-threat-report.html (дата звернення: 30.06.2022).

16. European union agency for cybersecurity. URL: https://www.enisa.europa.eu. (дата звернення: 30.06.2022).

**Курсивом зазначені джерела, що є в наявності в бібліотеці ДТЕУ*