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 ДТЕУ
(пост. п. 10 від «30» 06 2022 р.)
Ректор
_____ Анатолій МАЗАРАКІ

РОБОЧА ПРОГРАМА ПРАКТИЧНОЇ ПІДГОТОВКИ 1

освітній ступінь	**магістр**	/	master
галузь знань	**12 Інформаційні технології**	/	Information Technologies
спеціальність	**125 Кібербезпека**	/	Cybersecurity
освітня програма	**Безпека систем електронних комунікацій в економіці**	/	Security of electronic communications systems in the economy

Київ 2022

Автори: О.В. Криворучко, док. тех. наук, проф,
Л.О. Власенко, канд. тех. наук, доцент
А.М. Десятко, PhD, доцент
Ю.В. Костюк, ст. викл.
Т.В. Савченко, канд. тех. наук, доцент

Робочу програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «15» листопада 2021р., протокол № 12.

Рецензенти: Н.О. Котенко, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Б.Т. Бебешко, Senior Software Engineer, Softorino Inc.

РОБОЧА ПРОГРАМА
ПРАКТИЧНОЇ ПІДГОТОВКИ 1

освітній ступінь	**магістр**	/	master
галузь знань	**12 Інформаційні технології**	/	Information Technologies
спеціальність	**125 Кібербезпека**	/	Cybersecurity
освітня програма	**Безпека систем електронних комунікацій в економіці**	/	Security of electronic communications systems in the economy

ВСТУП

Проходження студентами практичної підготовки на суб'єктах господарської діяльності передбачається навчальними планами підготовки магістрів зі спеціальності 125 «Кібербезпека», освітньої програми (ОП) «Безпека систем електронних комунікацій в економіці».

Практична підготовка 1 студентів є складовою навчального плану підготовки здобувачів другого (магістерського) рівня вищої освіти та важливим етапом практичної підготовки фахівців, що проходить в один етап протягом 360 год.

Базами практики можуть бути суб'єкти господарської діяльності різних форм власності, видів господарської діяльності, організаційно-правового статусу, які є юридичними особами і функціонують на ринку не менше двох років та здійснюють виробничо-торговельну, науково-дослідницьку, інформаційну та інші види діяльності із широким застосуванням інформаційних технологій та комп'ютерної техніки.

Робочу програму практичної підготовки розроблено відповідно до: Закону України «Про вищу освіту», постанови Кабінету Міністрів України «Про затвердження Положення про порядок реалізації права на академічну мобільність», наказу МОН «Про запровадження у вищих навчальних закладах України Європейської кредитно-трансферної системи», інших нормативно-правових актів МОН України, положення про виробничу практику студентів вищих навчальних закладів України, затвердженого Міністерством освіти України, освітньо-професійної програми підготовки фахівців спеціальності 125 «Кібербезпека», ОП «Безпека систем електронних комунікацій в економіці», «Положення про проведення практичної підготовки здобувачів вищої освіти ДТЕУ», а також «Положення про організацію освітнього процесу студентів ДТЕУ».

Зміст практики відповідає вимогам стандарту вищої освіти ДТЕУ для підготовки магістрів зі спеціальності 125 «Кібербезпека», ОП «Безпека систем електронних комунікацій в економіці», а також враховує специфіку галузей економіки, в яких працюватиме випускник, основні завдання, види і зміст діяльності фахівця відповідної спеціальності, а також особливості суб'єктів господарської діяльності, які є базами практики.

Робоча програма практичної підготовки є основним навчально-методичним документом, який регламентує загальні положення щодо організації, порядку проведення та підсумків комплексної практики, визначає їх змістовну частину і тривалість проходження.

Робочу програму підготовлено відповідно до структурно-логічної схеми навчального процесу та вимог обов'язкової компоненти освітньо-кваліфікаційної характеристики фахівця підготовки магістрів зі

спеціальності 125 «Кібербезпека» ОП «Безпека систем електронних комунікацій в економіці».

Тривалість практики визначається діючими навчальними планами для здобувачів вищої освіти даного напряму підготовки.

Робоча програма практичної підготовки складається з таких розділів:

1. Мета, завдання та результати практики, її місце в освітньому процесі.
2. Зміст практики.
3. Індивідуальні завдання.
4. Список рекомендованих джерел.

Розділ 1
МЕТА, ЗАВДАННЯ ТА РЕЗУЛЬТАТИ ПРАКТИЧНОЇ ПІДГОТОВКИ 1, ЇЇ МІСЦЕ У ОСВІТНЬОМУ ПРОЦЕСІ

Робоча програма практичної підготовки 1 відповідає вимогам стандарту вищої освіти ДТЕУ зі спеціальності 125 «Кібербезпека» для здобувачів вищої освіти другого (магістерського) рівня, ОП «Безпека систем електронних комунікацій в економіці» і забезпечує здійснення професійної діяльності на посадах фахівців з організації інформаційної безпеки.

Практична підготовка 1 проходить після ІІ семестру (табл. 1).

Таблиця 1

Розподіл практичної підготовки 1
студентів спеціальності 125 «Кібербезпека»
ОП «Безпека систем електронних комунікацій в економіці»

№ з/п	***Види практики***	***Термін (семестр)***	***Тривалість, год.***
1.	Практична підготовка 1	ІІ	360

Головною метою практичної підготовки 1 є забезпечення єдності теоретичного та практичного навчання студентів, поглиблення та закріплення студентами теоретичних знань, оволодіння ними сучасними технологіями та формами організації праці у сфері їхньої майбутньої професії та набуття ними практичних навиків і компетентностей, а також досвіду самостійної професійної діяльності, формування здатності самостійно систематично навчатися та вдосконалювати свої знання у вирішенні нових викликів в сфері кібербезпеки та захисту інформації. Також за мету практика ставить формування у студентів на базі знань, які

одержані у вищому навчальному закладі, професійних умінь і навичок щодо прийняття самостійних рішень під час професійної діяльності в реальних ринкових умовах; поглиблення та закріплення теоретичних знань з фахових дисциплін; ознайомлення з засобами забезпечення інформаційної безпеки і захисту інформації, що використовуються суб'єктами господарської діяльності; вивчення нормативної бази, що регулює забезпечення інформаційної безпеки і захисту інформації, що використовується та обробляється даним суб'єктом господарської діяльності; опрацювання наукової, періодичної літератури й методичних матеріалів з питань, що підлягають опрацюванню.

Завданнями практики є:

1. Закріплення, поглиблення та доповнення теоретичних знань, які набуваються при засвоєнні курсів: «Безпека мережевої та SMART-інфраструктури», «Етичний хакінг», «Технології безпеки безпроводових та мобільних мереж», «Технології безпеки Web-ресурсів».

2. Удосконалення професійно-практичної підготовки студентів шляхом розвитку в них компетентностей, передбачених освітньою програмою, на наявній матеріально-технічної базі практичної підготовки.

3. Збір матеріалів за темою кваліфікаційної роботи, зокрема, оцінювання стану системи захисту суб'єкта господарської діяльності.

Після проходження практичної підготовки студент повинен

знати:

- методи та засоби формування політики безпеки;
- засади проектування захисту баз даних;
- стандарти та методи управління інцидентами;
- засади побудови комплексної системи захисту інформації;
- архітектури комп'ютерних мереж та протоколів для виявлення аномалій;
- методи тестування на проникнення та аудиту безпеки програм;
- технологію проектування системи безпеки робочого місця користувача;
- структуру та зміст технічного, програмного, програмно-апаратного забезпечення безпеки даних у системі;
- алгоритм реагування на кіберінциденти та відновлення роботи систем після атаки;
- основи законодавства щодо кібербезпеки та обмежень відповідно до нього.

вміти:

- аналізувати конкретну предметну область на вразливості;
- обґрунтовано обирати метод (структурний, процесний, статистичний, системний) дослідження стану безпеки даних в організації;

- виконувати моделювання стану предметної області за завданням з використанням інструментів для моделювання, які реалізують обраний метод;
- робити якісну постановку конкретного завдання на формування профілю безпеки;
- проводити аналіз можливих загроз на інформаційні ресурси організації, визначити критичні місця в мережі організації;
- аналізувати програмний код на наявність вразливостей та використання їх для атак;
- моделювати захист бази даних;
- проектувати профіль безпеки для окремого користувача;
- складати звіт з аналізу поточного стану безпеки окремого користувача в системі;
- аналізувати нові кіберзагрози та визначати їхні можливі наслідки;
- розробляти та впроваджувати заходи забезпечення мережевої безпеки.

здобути навички:

- використання системного підходу щодо формування профілю безпеки, аналізу можливих загроз, технічних засобів протидії;
- обґрунтування необхідності та можливості удосконалення або розробки нового модуля автоматизації оброблення інформації;
- спілкування з адміністративним апаратом організації для пошуку відповідей за питаннями практики;
- роботи в команді для реалізації заходів з підвищення кібербезпеки.

Практична підготовка посилює та закріплює всі компетентності та програмні результати навчання студентів, передбачених ОП, а також передбачає безперервність та послідовність отримання потрібного обсягу практичних знань і умінь відповідно до освітнього ступеня «магістр».

Згідно з обов'язковою компонентою освітньої характеристики фахівця зі спеціальності 125 «Кібербезпека», ОП «Безпека систем електронних комунікацій в економіці», підготовка магістра зорієнтована на одержання студентами кваліфікаційного рівня, що забезпечує здійснення професійної діяльності на посадах фахівців з питань безпеки (інформаційно-телекомунікаційних технологій), сфери захисту інформації, реагування на інциденти кібербезпеки, з криптографічного, технічного захисту інформації, організації та проведення тестування на проникнення, з планування політики та стратегії кібербезпеки, із кібердосліджень та розробок систем безпеки тощо. Ця особливість позначається на організації практичної підготовки магістрів за даним напрямом, оскільки практика на відповідних суб'єктах господарської діяльності є передумовою форму-

вання навичок і ознайомлення із виконанням функцій фахової і керівної роботи.

Очікуваний результат практичної підготовки 1: підвищення компетентності фахівця з кібербезпеки, що володіє сформованими на основі знань, умінь, навичок і практичного досвіду компетенціями виконувати встановлені для другого (магістерського) рівня вищої освіти спеціальності 125 «Кібербезпека», ОП «Безпека систем електронних комунікацій в економіці».

Навчальним планом магістра передбачається проходження практики на провідних суб'єктах господарської діяльності України різних форм власності. При проходженні практичної підготовки студентами спеціальності 125 «Кібербезпека», ОП «Безпека систем електронних комунікацій в економіці» робочою програмою практичної підготовки 1 передбачено виконання низки дослідницьких задач, встановлених індивідуальним завданням студента, зокрема, збір даних для написання статті та виконання кваліфікаційної роботи. Практика студентів є невід'ємною складовою частиною процесу підготовки фахівців у вищих навчальних закладах і проводиться на оснащених відповідним чином базах навчальних закладів, а також на сучасних суб'єктах господарської діяльності і в організаціях різних галузей господарства, торгівлі і державного управління.

Розділ 2
ЗМІСТ ПРАКТИЧНОЇ ПІДГОТОВКИ

Відповідно до структурно-логічної схеми підготовки магістра практична підготовка 1 є складовою частиною робочого навчального плану магістра зі спеціальності 125 «Кібербезпека», ОП «Безпека систем електронних комунікацій в економіці».

Практична підготовка 1 проводиться у II семестрі I курсу після складання студентами іспитів, тривалість практики 360 год (12 кредитів ЄКТС) — на суб'єкті господарської діяльності.

Здобувач вищої освіти має виконувати обов'язки фахівця з організації інформаційної безпеки (за Класифікатором професій України ДК 003:2010: 2139.2), а саме:

– фахівця з питань безпеки;
– фахівця захисту інформації;
– фахівця з реагування на інциденти кібербезпеки;
– фахівця сфери захисту інформації;
– фахівця з криптографічного захисту інформації;
– фахівця з тестування систем захисту;
– фахівця з підтримки інфраструктури кіберзахисту.

В перший день проходження практики на суб'єкті господарської діяльності, об'єкті практики, студент повинен пройти інструктаж з техніки безпеки на робочому місці та пожежної безпеки, ознайомитись з правилами охорони праці при експлуатації персональних комп'ютерів й інших технічних засобів та з відповідальністю за їх порушення.

При порушенні студентами-практикантами трудової дисципліни, правил внутрішнього розпорядку, техніки безпеки та інших норм наказом керівника суб'єкта господарської діяльності на них може бути накладене стягнення, про що повідомляється декан факультету та завідувач кафедри.

Значне місце у практичній підготовці посідає ознайомлення студентів з функціональними обов'язками службових осіб з профілю професійної діяльності, функціями, правами та обов'язками; відпрацювання на посадах, що заміщуються фахівцями, відповідно до їх спеціальності та освітнього рівня, технологією виконання основних інформаційно-технологічних процесів, які здійснюються на суб'єкті господарської діяльності певного типу та організаційно-правової форми господарювання, і передбачених кваліфікаційними характеристиками фахівця.

Орієнтовний план-графік практичної підготовки 1 з розподілом за годинами представлений в таблиці 2.

Таблиця 2

Орієнтовний план-графік практичної підготовки 1 з розподілом за годинами

№ з/п	Зміст роботи	Кількість годин
1	2	3
1.	Огляд програми практики	2
2.	Проходження інструктажу з техніки безпеки, пожежної безпеки	2
3.	Ознайомлення з суб'єктом господарської діяльності - об'єктом практики	4
4.	Виконання індивідуального завдання:	
	Тема 1: Дослідження суб'єкта господарської діяльності та аналіз його системи безпеки	60
	Тема 2: Проведення аналізу роботоспроможності безпроводових та/або мобільних мереж суб'єкта господарської діяльності і пошук в них вразливостей	60
	Тема 3: Оцінка вразливостей Web-ресурсів суб'єкта господарської діяльності	70

	Тема 4: Дослідження загроз, ризиків та вразливостей, пов'язаних зі зростаючою кількістю підключених пристроїв та систем	70
	Тема 5: Аналіз безпеки інформаційних систем, програм та/або мереж суб'єкта господарювання на стійкість до атак	70
5.	Аналіз результатів практичної підготовки	10
6.	Оформлення доповіді за результатами виконання індивідуального завдання	10
7.	Захист результатів практичної підготовки 1	2
	Всього годин:	360

Огляд програми практики

Мета, завдання та вимоги до проходження практики. Огляд програми практики.

Обговорення календарного плану проходження практики. Правила оформлення щоденника практики. Правила підготовки доповіді за результатами виконання індивідуальних завдань.

Проходження інструктажу з техніки безпеки, пожежної безпеки

Організація охорони праці на суб'єкті господарської діяльності. Обов'язки працівника виконувати вимоги нормативних актів про охорону праці. Громадський контроль за дотриманням законодавства про охорону праці. Відповідальність за порушення законодавчих та інших нормативних актів про охорону праці. Види інструктажів з питань охорони праці та порядок їх проведення. Правила охорони праці при експлуатації персональних комп'ютерів, комп'ютерних мереж та периферійної та спеціальної техніки.

Ознайомлення з суб'єктом господарської діяльності – об'єктом практики

Визначення назви, юридичної та фактичної адреси суб'єкти господарської діяльності, форми власності та типу діяльності.

Визначення нормативно-правової бази роботи суб'єкти господарської діяльності.

Правила внутрішнього трудового розпорядку для співробітників організації. Ознайомлення з робочим місцем.

Виконання індивідуального завдання

Завдання для практикантів встановлює керівник практики від суб'єкта господарської діяльності згідно з виробничими функціями,

типовими завданнями діяльності та вміннями, які повинен мати магістр зі спеціальності 125 «Кібербезпека» ОП «Безпека систем електронних комунікацій в економіці».

Особисте індивідуальне завдання є унікальним для кожного студента, визначається керівником практики. Індивідуальні завдання виконують студенти самостійно у супроводженні керівника практики.

Аналіз результатів практичної підготовки

Студент разом з керівником практики від суб'єкта господарської діяльності згідно з індивідуальним завданням оцінюють результати практики.

Оформлення доповіді за результатами виконання індивідуального завдання

Студент самостійно готує доповідь за результатами виконання індивідуального завдання.

Захист результатів практичної підготовки

Здобувач освіти захищає результати проходження практичної підготовки 1 на кафедрі інженерії програмного забезпечення та кібербезпеки перед комісією, що призначена завідувачем кафедри.

По закінченні практики студент надає заповнений щоденник практики, в якому детально описано всі етапи виконання завдання та представляє на захист результат виконання завдання.

Керівник практики від суб'єкти господарської діяльності, за умови позитивної оцінки виконання індивідуального завдання, готує характеристику на студента, викладає її в щоденнику практики, де оцінює виконання програми практики, індивідуального завдання. Після отримання затверджених печаткою суб'єкти господарської діяльності характеристики та рецензії за підписом керівника з бази практики студент подає щоденник на кафедру для реєстрації та перевірки керівником від університету.

Керівник практики від кафедри розглядає й оцінює щоденник та індивідуальне завдання студента, надає рекомендації щодо допущення до захисту.

Захист практики приймає комісія, яка призначається завідувачем кафедри, відповідно до діючої в університеті системи оцінювання знань здобувачів вищої освіти. Здобувач готує до захисту опис та обґрунтування технічного завдання, демонструє програмну розробку (програмний продукт). За результатами захисту виставляється залік. Оцінка за практику вноситься в заліково-екзаменаційну відомість і в залікову книжку студента.

Критеріями оцінювання успішності проходження практики є:

- ✓ вчасність захисту;
- ✓ відповідність оформлення щоденника вимогам університету і кафедри;
- ✓ повнота та глибина розробки окремих питань індивідуального завдання;
- ✓ наявність та зв'язаність чітко сформульованих задач, що будуть розв'язані у дипломній роботі;
- ✓ творчий підхід до виконання завдань;
- ✓ ініціативність у виконанні завдань практики

При незадовільній оцінці – кафедра вносить пропозицію деканату про відрахування студента.

Здобувач, який не виконав програми практики з об'єктивних причин, може бути надано дозвіл пройти практику повторно на умовах, визначених кафедрою.

Розділ 3
ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Практична підготовка 1 на суб'єкті господарської діяльності передбачає послідовне виконання індивідуальних завдань на основі типових завдань, дослідження та впровадження технологій пошуку та менеджменту інформації, зокрема використання методів ідентифікації, класифікації, індексації та подання інформації в умовах дослідження нових комп'ютерних інформаційних технологій за допомогою програмних і технічних засобів, локальних і глобальних комп'ютерних мереж, мережі Інтернет.

Напрями завдань:

Тема 1. Дослідження суб'єкта господарської діяльності та аналіз структури його системи безпеки.

Навести функціональну схему організації (суб'єкта господарської діяльності) з вказівкою підпорядкування головних композиційних складових та функцій кожної з них за допомогою засобу моделювання. Окремо вказати місце підрозділу, де безпосередньо проходитиме практика та інформаційні зв'язки цього підрозділу з ближнім оточенням. Навести структуру системи безпеки суб'єкта господарської діяльності, склад посадових осіб конкретного підрозділу та їх функції.

Тема 2. Проведення аналізу роботоспроможності безпроводових та/або мобільних мереж суб'єкта господарської діяльності і пошук в них вразливостей.

Дослідження імовірних загроз мережі, аналіз інструментів для сканування мережі на вразливості, тестування на проникнення в систему через мережу. Аналіз вразливостей, пов'язаних з мобільними платформами, та їх впливу на безпеку. Тестування додатків на вразливості. Вивчення атак на Wi-Fi та Bluetooth мережі, аналіз їх наслідків та розробка заходів захисту.

Тема 3. Оцінка вразливостей Web-ресурсів суб’єкта господарської діяльності.

Методи аналізу вразливостей в веб-додатках, таких як SQL-ін'єкції, міжсайтові скрипти, переповнення буфера, та розробка методів захисту від них.

Тема 4. Дослідження загроз, ризиків та вразливостей, пов'язаних зі зростаючою кількістю підключених пристроїв та систем.

Дослідити та проаналізувати сучасні підходи до забезпечення безпеки в мережевій та SMART-інфраструктурі. Скласти рекомендації та стратегії для забезпечення цілісності, конфіденційності та доступності даних та функцій в мережевій чи/та SMART-інфраструктурі. Провести аналіз сучасних методів шифрування, аутентифікації та контролю доступу для захисту мережевих з'єднань та пристроїв. Визначення можливості виявлення та реагування на кібератаки та вразливості в реальному часі. Дослідження можливих загроз та ризиків при використанні хмарних сервісів, аналіз методів шифрування та контролю доступу.

Тема 5. Аналіз безпеки інформаційних систем, програм та/або мереж суб’єкта господарювання на стійкість до атак.

Огляд можливих ризиків та загроз від підключених пристроїв. Вивчення різних видів мережевих атак. Визначення оптимальних методів захисту від DDoS згідно з типами атак. Дослідження методів детекції та виправлення вразливостей в програмному коді. Аналіз методів соціальної інженерії та їх впливу на співробітників суб’єкта господарювання. Дослідження типових загроз та можливих ризиків в хмарних середовищах.

Виконання особистого індивідуального завдання.

Індивідуальне завдання є однією з форм набуття фахових компетентностей, яка має на меті поглиблення, узагальнення та закріплення знань, які студенти отримали у процесі теоретичного навчання, та застосування цих знань в практичній діяльності.

Індивідуальне завдання є особистим для кожного студента, визначається керівником практики. Індивідуальні завдання виконують студенти самостійно у супроводженні керівника практики. Як правило, індивідуальні завдання виконуються окремо кожним студентом. У тих випадках,

коли завдання мають комплексний характер, до їх виконання можуть залучатися кілька студентів.

Індивідуальні завдання, що відносяться до практичної підготовки 1 повинні відповідати темі та змісту кваліфікаційної роботи магістра спеціальності 125 Кібербезпека ОП «Безпека систем електронних комунікацій в економіці».

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основна література

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В.Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний, Н.В. Лукова-Чуйко / – К. : ДУТ – КНУ, 2016. – 178 с.
2. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.: ДУТ, 2015. – 345 с.
3. *Бабенко Л.П. Основи програмної інженерії: навч. посіб./ Л.П. Бабенко Л.П., К.М. Лавріщева К.М. – К.: Т-во «Знання», 2001. – 269 с.*
4. *Вовчак І.С. Інформаційні системи та комп'ютерні технології в менеджменті: Навч. Посібник / І.С. Вовчак – Тернопіль: "Картбланш", 2001. – 286 с.*
5. *Гужва, В.М. Інформаційні системи в міжнародному бізнесі: Навч. посібник / В.М. Гужва, А.Г. Постєвой. – К. : КНЕУ, 2002. – 458 с.*

Додаткова література

6. Остапов С.Е., Євсеєв С.П., Король О.Г., Технології захисту інформації – Чернівці: Видавничий дім «Родовід», 2014. – 471 с.
7. Кавун С.В. Інформаційна безпека. – Харків : ХНЕУ, 2013. – 213 с.
8. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 435 с.
9. *Гребельник О.П. Основи зовнішньоекономічної діяльності: Підручник / О.П. Гребельник – К.: Центр учбової літератури, 2008. – 432 с.*
10. Грещак М.Г. Економіка суб'єкти господарської діяльності: підручник / М.Г. Грещак, В.М. Колот, А.П. Наливайко та ін.; за заг. ред. С.Ф. Покропивного. – 2-ге вид. – К. : КНЕУ, 2001. – 528 с.
11. *Гужва В.М. Інформаційні системи і технології на суб'єктах господарської діяльності / В.М. Гужва – К.: КНЕУ,2001. – 400с.*

12. *Демідов П.Г. Комп'ютерні тренінгові системи в економіці: Навч.-метод. посіб. / П.Г. Демідов – К.: Київ. нац.. торг.-екон. ун-т, 2005. – 241 с.*
13. *Степанова Я.М. Методи і засоби передачі даних. Підручник. / Я.М. Степанова, В.Я.Рассамакін – К. ВЦ ДТЕУ, 2006, – 252 с.*
14. *Кавун С.В. Системи штучного інтелекту: навч. посіб./ С.В. Кавун, В.М. Коротченко – Харьків: ХНЕУ, 2007. – 320с.*
15. *Мінухін С.В. Комп'ютерні мережі. Загальні принципи функціонування комп'ютерних мереж: навч. посіб. / С.В. Мінухін, С.В. Кавун, С.В. Знахур. — Харків : ХНЕУ, 2008. — 208 с.*
16. *Тарасов, О.В. Використання мови SQL для роботи з сучасними системами керування базами даних. Практикум з навчальної дисципліни "Організація баз даних та знань" [Текст] : навч.-практ. посіб. / О.В. Тарасов, М.Ю. Лосєв, В.В. Федько. – Харків : ХНЕУ, 2013. – 347 с.*
17. *Федько, В.В. Організація баз даних та знань: навч.-практ. посіб. для самост. підготов. студ. / В.В. Федько, О.В. Тарасов, М.Ю. Лосєв. – Харків: ХНЕУ, 2013. – 198 с.*
18. Єсін В.І. Безпека інформаційних систем і технологій : навчальний посібник / В.І. Єсін, О.О. Кузнецов, Л.С. Сорока. – Х.: ХНУ імені В.Н. Каразіна, 2013. – 632 с.
19. Закон України «Про інформацію» від 02.10.1992 № 2657-XII.
20. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР.
21. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373.
22. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
23. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96.
24. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.
25. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
26. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

27. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

Інтернет-ресурси

28. Положення про організаційно-технічну модель кіберзахисту. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text
29. Порядок реагування на кіберінциденти та кібератаки. URL: http://surl.li/klznf
30. Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами». URL: http://surl.li/klzmp

** Курсивом виділені назви видань, які є в наявності в бібліотеці ДТЕУ*