КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ 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 ФІТ
протокол № 6 від 25.01.2022
Декан _____ Харченко О.А.

РОБОЧА ПРОГРАМА ПРАКТИЧНОЇ ПІДГОТОВКИ 2

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 2021

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 2021 р., 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 2

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

Практика студентів є невід'ємною частиною процесу підготовки фахівців та складовою навчального плану з базової освіти і важливим етапом наскрізної практичної підготовки.

Практична підготовка 2 проводиться в межах КНТЕУ, в органах державного управління та місцевого самоврядування, на суб'єктах господарської діяльності національної економіки, ІТ-індустрії всіх форм власності, в установах та організаціях, діяльність яких фінансується за рахунок коштів державного та/або місцевих бюджетів.

Базами практики можуть бути суб'єкти господарської діяльності різних форм власності, організації різних галузей національного господарства, органи державної влади, наукові установи і організації, діяльність яких безпосередньо пов'язана з інформаційними технологіями або захистом інформації, або в структурі яких є підрозділи що забезпечують інформаційну безпеку або в штаті є посада фахівця в галузі інформаційних технологій.

Метою практичної підготовки 2 є опанування студентами сучасних методів та форм організації їх майбутньої професії, формування на базі отриманих в КНТЕУ знань, умінь і навичок можливостей прийняття самостійних рішень під час конкретної роботи та в реальних ринкових і виробничих умовах; виховання потреби систематично оновлювати свої знання, творчо застосовувати їх в практичній діяльності.

Практична підготовка 2 студентів передбачає безперервність та послідовність її проведення при одержанні необхідного обсягу практичних навичок, відповідно до освітнього ступеня магістра.

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 КНТЕУ, а також Положення про організацію освітнього процесу студентів КНТЕУ.

Зміст практики відповідає вимогам стандарту вищої освіти КНТЕУ для освітнього ступеня магістр зі спеціальності 125 «Кібербезпека», ОП «Безпека систем електронних комунікацій в економіці», а також враховує специфіку ІТ-галузі, в яких працюватиме випускник, основні завдання, види і зміст діяльності фахівця відповідної спеціалізації, а також особливості суб'єктів господарської діяльності, які є базами практики.

Тривалість практичної підготовки 2 визначається діючими навчальними планами для студентів даного напряму підготовки та проводиться в один етап протягом 90 год. (3 кредити ЄКТС).

Розділ 1
МЕТА, ЗАВДАННЯ ТА РЕЗУЛЬТАТИ ПРАКТИЧНОЇ ПІДГОТОВКИ 2, ЇЇ МІСЦЕ У ОСВІТНЬОМУ ПРОЦЕСІ

Робоча програма практичної підготовки 2 відповідає вимогам стандарту вищої освіти КНТЕУ для освітнього ступеня магістрів зі спеціальності 125 «Кібербезпека», ОП «Безпека систем електронних комунікацій в економіці» і забезпечує здійснення професійної діяльності на посадах фахівців із організації інформаційної безпеки.

Практична підготовка 2 проходить в ІІІ семестрі (табл. 1).

Таблиця 1

Розподіл практичної підготовки 2 студентів спеціальності 125 «Кібербезпека», ОП «Безпека систем електронних комунікацій в економіці»

№ з/п	*Види практики*	*Термін (семестр)*	*Тривалість, год.*
1.	Практична підготовка 2	ІІІ	90 год. (3 кредити ЄКТС)

Головною метою практичної підготовки 2, що є завершальним етапом навчання на випускному курсі, спрямованим на завершення написання магістерської роботи, узагальнення та поглиблення їхніх фахових компетентностей – знань, практичних умінь та навичок, забезпечення єдності теоретичного та практичного навчання здобувачів, поглиблення та закріплення ними теоретичних знань та набуття практичних навиків і компетентностей, а також досвіду самостійної

професійної діяльності. Вона сприяє накопиченню професійного досвіду та готує студентів до самостійної трудової діяльності в майбутньому. 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 із засобами забезпечення інформаційної безпеки і захисту інформації, що використовуються суб'єктом 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.

Завданням практики є:

- підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки;
- вивчення організаційно-функціональної структури, складу і характеристик систем захисту інформації;
- вироблення навиків творчого підходу до вирішення теоретичних і практичних задач проектування, конструювання, створення і випробування елементів і систем захисту інформації;
- збір матеріалів, необхідних для виконання кваліфікаційної роботи, вивчення нових досягнень за темою кваліфікаційної роботи, огляд існуючих рішень виявленої та сформульованої проблеми, вироблення правильного алгоритму виконання досліджень і впровадження отриманих результатів;
- вироблення вміння адекватної оцінки головних техніко-економічних показників у відповідності до чинних нормативно-технічних документів;
- вивчення заходів з техніки безпеки, охорони праці, протипожежної безпеки, охорони навколишнього середовища та цивільної оборони.

Внаслідок проходження переддипломної практики студент повинен

знати:

- сучасні засоби фізичного захисту інформації;
- методи реалізації НСД;
- методи реалізації захисту інформації від стороннього деструктивного впливу;
- сучасні вимоги щодо захисту інформації від НСД;
- засоби захисту інформації в ІКС від витоку її технічними каналами;

вміти:

- проводити аналіз проблеми безпеки інформації за науково-технічними джерелами;
- проводити оцінку стану захищеності ІС;
- розробляти вимоги щодо захисту інформації від НСД, застосовувати засоби захисту інформації в ІКС;

здобути навички:

- застосування фізичних засобів захисту інформації в ІКС;
- аналізу захищеності ІС;
- робити обґрунтовані висновки щодо необхідності модернізації і розвитку системи інформаційної безпеки;
- розробляти пропозиції по модернізації системи інформаційної безпеки;
- розробляти рекомендаційні заходи щодо поліпшення безпекових заходів на суб'єкті господарювання на основі проведеного аудиту.

Практична підготовка 2 студентів 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 формування навичок і ознайомлення із виконанням функцій фахової і керівної роботи.

Очікуваний результат практичної підготовки 2: 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 зі спеціальності 125 «Кібербезпека» ОП «Безпека систем електронних комунікацій в економіці».

Отримані під час проходження практичної підготовки 2 знання та досвід, здобувачі вищої освіти спрямовують на науково-дослідну роботу та при підготовці доповідей до наукових студентських конференцій,

виступів на науково-практичних семінарах, а також при написанні кваліфікаційної роботи.

Здобувач також має продемонструвати володіння англійською мовою, включаючи спеціальну термінологію, для реалізації розробленої програми в англомовній версії.

Розділ 2
ЗМІСТ ПРАКТИЧНОЇ ПІДГОТОВКИ

Відповідно до структурно-логічної схеми підготовки здобувачів другого (магістерського) рівня вищої освіти, практична підготовка 2 є складовою частиною робочого навчального плану магістра зі спеціальності 125 «Кібербезпека» ОП «Безпека систем електронних комунікацій в економіці».

Практична підготовка 2 проводиться в ІІІ семестрі на другому курсі, тривалість практики 90 год. (3 кредити ЄКТС) – на суб'єктах господарської діяльності – об'єктах практики.

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

– фахівець з питань безпеки;
– фахівець захисту інформації;
– фахівець з реагування на інциденти кібербезпеки;
– фахівець сфери захисту інформації;
– фахівець з криптографічного захисту інформації;
– фахівець з тестування систем захисту;
– фахівець 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 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 2 з розподілом за годинами представлений в таблиці 2.

Таблиця 2

Орієнтовний план-графік практичної підготовки 2 з розподілом за годинами

№ з/п	*Зміст роботи*	*Кількість годин*
1	2	3
1.	Огляд програми практики	1
2.	Проходження інструктажу з техніки безпеки, пожежної безпеки	2
3.	Ознайомлення з суб'єктом господарської діяльності – об'єктом практики	2
4.	Виконання індивідуального завдання:	
	ІЗ1: Аналіз інформаційної складової суб'єкта господарської діяльності, ідентифікація об'єктів, які потребують захисту: програмне, апаратне забезпечення, інформація з обмеженим доступом; розпізнання можливих загроз та їх аналіз.	10
	ІЗ2: Оцінка комплексу заходів забезпечення інформаційної безпеки суб'єкта господарської діяльності. Проведення аудиту для виявлення слабких місць та вразливостей в системах захисту організаційної, технічної та програмної складових структури інформаційної системи суб'єкта господарської діяльності (об'єкта практики).	10
	ІЗ3: Розроблення вимог щодо вдосконалення системи захисту інформації, підвищення рівня захищеності інформації в інформаційних системах суб'єкта господарської діяльності (об'єкта практики) на основі проведеного аудиту.	20
	ІЗ4: Розробка рекомендацій щодо вдосконалення системи захисту інформації, підвищення рівня захищеності інформації в інформаційних системах суб'єкта господарської діяльності (об'єкта практики) на основі проведеного аудиту.	30

№ з/п	*Зміст роботи*	*Кількість годин*
	І35: Збір матеріалів: ✓ випускової кваліфікаційної роботи; ✓ підготовки доповідей на наукові студентські конференції; ✓ написання наукових статей.	Протягом всього часу проходження практичної підготовки 2
5.	Аналіз результатів практичної підготовки	5
6.	Підготовка доповіді за результатами виконання індивідуального завдання	8
7.	Захист результатів практичної підготовки 2	2
	Всього годин:	90

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 техніки.

Ознайомлення з суб'єктом господарської діяльності-об'єктом практики.

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

Визначення нормативно-правової бази роботи суб'єкта 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».

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

Оформлення доповіді за результатами виконання індивідуального завдання.

Студент самостійно готує доповідь за результатами виконання індивідуального завдання.

Захист результатів виробничої практики.

Студент захищає результати проходження практичної підготовки 2 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'єкта 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'єкта 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, дає надає рекомендації щодо допущення до захисту.

Після закінчення терміну практичної підготовки здобувачі вищої освіти складають залік за наявності відповідним чином оформленого щоденника, підписаного та завіреного печатками або кваліфікованими електронними підписами, отриманого сертифіката від бази практики, який свідчить про набуття практичних навичок. 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 позитивній оцінці за практику та за наявності позитивних оцінок по всіх дисциплінах навчального плану студент допускається до написання дипломної роботи.

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

Здобувач, який не виконав програму практики або не встиг скласти залік у визначені терміни без поважних причин, за поданням кафедри та деканату відраховується з університету.

Розділ 3
ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Індивідуальні завдання включені у робочу програму з метою надбання здобувачами вищої освіти під час практики умінь та навичок самостійного розв'язання виробничих, наукових або організаційних завдань з урахуванням вимог замовників-роботодавців. Виконання індивідуальних завдань робить проходження практики більш конкретним і цілеспрямованим.

Практична підготовка 2 на суб'єкті господарської діяльності передбачає послідовне виконання індивідуальних завдань на основі типових завдань, дослідження та впровадження технологій пошуку вразливостей та слабких місць в системі безпеки суб'єкта господарської діяльності, 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:

І31. Аналіз інформаційної складової суб'єкта господарської діяльності, ідентифікація об'єктів, які потребують захисту: програмне, апаратне забезпечення, інформація з обмеженим доступом; розпізнання можливих загроз та їх аналіз.

Для виконання цього завдання необхідно: 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 склад посадових осіб конкретного підрозділу та їх функції.

Проаналізувати систему управління суб'єктом господарської діяльності і визначити організації управління, які підтримуються ЦІТ. Для

цього необхідно: ознайомитись і дослідити наявний інформаційний процес, провести його аналіз із урахуванням особливостей безпекової складової; вивчити основні потреби користувачів інформації та визначити інформаційні потоки об’єктів, пов’язаних у своїй діяльності з суб’єктом господарської діяльності з урахуванням існуючих безпекових заходів.

Визначити структуру інформаційної системи суб’єкта господарської діяльності, класифікувати ІС. Визначити нормативно-правову базу організації ІС суб’єкта господарської діяльності-об’єкта практики. Дослідити організацію інформаційної діяльності суб’єкта господарської діяльності та електронного документообігу. Проаналізувати організацію інформаційних потоків між структурними підрозділами суб’єкта господарської діяльності. Виділити об’єкти, які потребують захисту.

І32. Оцінка комплексу заходів забезпечення інформаційної безпеки суб’єкта господарської діяльності. Проведення аудиту для виявлення слабких місць та вразливостей в системах захисту організаційної, технічної та програмної складових структури інформаційної системи суб’єкта господарської діяльності.

Щоб виконати дане завдання потрібно:

Після проведення аналізу суб’єкта господарської діяльності, дослідження його інформаційної системи, інформаційних потоків, які в ньому функціонують та визначення об'єктів, що потребують захисту, необхідно провести аналіз програмного та апаратного забезпечення, що використовуються для забезпечення його безпеки. Також вони ознайомлюються і детально вивчають інженерно-технічні рішення, реалізовані на суб’єкті господарської діяльності.

На цьому етапі також необхідно: проаналізувати нормативні документи технічного захисту інформації; виконати аналіз основних напрямків технічного захисту інформації в автоматизованих системах; проаналізувати основні загрози за результатом їх впливу на інформацію; навести політику безпеки інформації для об’єкта управління; розглянути комплекс заходів захисту та об’єкти комп’ютерної системи; дати визначення несанкціонованого доступу; охарактеризувати модель порушника; навести основні принципи забезпечення захисту інформації, нормативних, розпорядчих, організаційних тощо документів, які регламентують забезпечення безпеки інформації на суб’єкті господарської діяльності. Зокрема, інструкцій, які встановлюють обов'язки, права та відповідальність персоналу.

На основі проведеного аналізу робляться висновки щодо слабких місць в системах захисту та вразливостей в інформаційній системі.

ІЗ3. Розроблення вимог щодо вдосконалення системи захисту інформації, підвищення рівня захищеності інформації в інформаційних системах суб'єкта господарської діяльності (об'єкта практики) на основі проведеного аудиту.

На основі проаналізованої структури інформаційної системи, особливостей організації функціонування інформаційних потоків, особливостей організації мереж, технічних засобів, які використовуються на суб'єкті господарської діяльності, нормативно-правової бази виявлених можливих слабких місць та загроз в системі захисту необхідно розробити вимоги щодо вдосконалення захисту інформації та/або підвищення рівня її захищеності.

ІЗ4: Розробка рекомендацій щодо вдосконалення системи захисту інформації, підвищення рівня захищеності інформації в інформаційних системах суб'єкта господарської діяльності (об'єкта практики) на основі проведеного аудиту.

Щоб виконати дане завдання потрібно: здобувачами вищої освіти сформулювати власні пропозиції щодо покращення безпекової складової на суб'єкті господарської діяльності. Ці пропозиції повинні бути спрямовані на вдосконалення наявної системи захисту інформації, на підвищення безпеки інформаційних систем та інших аспектів. Якщо на об'єкті практики система захисту інформації відсутня, то практикант може запропонувати кроки для її впровадження.

Під час цього етапу важливо акцентувати увагу на таких напрямках забезпечення безпеки інформації:

- ✓ програмний захист;
- ✓ технічний захист;
- ✓ захист телекомунікаційних мереж та ін.
- ✓ організаційний, нормативно-правовий захист, та ін.

Передбачено, що замість підготовки рекомендацій здобувачі вищої освіти можуть запропонувати власні рішення для підвищення рівня безпеки, наприклад, самостійно розроблені програмні модулі, Web-додатки, технічні системи і т.д.

Інд ІЗ5. Збір матеріалів:

- ✓ випускової кваліфікаційної роботи;
- ✓ підготовки доповідей на наукові студентські конференції;
- ✓ написання наукових статей.

Матеріали, отримані студентом, при проходженні практичної підготовки 2 можуть бути використані для виконання випускової кваліфікаційної роботи, для підготовки доповідей, статей тощо (за узгодженням з кафедрою та базою практики).

Для цього необхідно:

- ✓ зібрати та опрацювати необхідні аналітичні матеріали для виконання дослідницької частини магістерської роботи;
- ✓ вивчити на практиці сучасні методи реалізації несанкціонованого доступу (НСД) та захисту інформації від стороннього впливу;
- ✓ вивчити специфіку інформаційних потоків конкретного об'єкта, що підлягає захисту;
- ✓ розробити вимоги щодо підвищення рівня захищеності інформації в інформаційній системі суб'єкта господарської діяльності;
- ✓ розробити рекомендації щодо підвищення рівня захищеності інформації в інформаційній системі суб'єкта господарської діяльності.

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 КНТЕУ, 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 КНТЕУ*