



Вищий навчальний заклад
«НАЦІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ»
Факультет економіки та інформаційних технологій
Кафедра фінансів, обліку та фундаментальних економічних дисциплін

ЗАТВЕРДЖЕНО

Декан факультету економіки та
інформаційних технологій


Ю.М. Неговська

РОБОЧА ПРОГРАМА

ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА

(назва навчальної дисципліни)

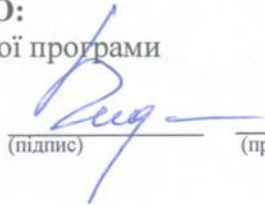
підготовки _____ другий (магістерський) _____
(назва рівня вищої освіти)
галузі знань _____ 08 «Право» _____
(шифр і назва галузі знань)
Спеціальності _____ 081 «Право» _____
(код і найменування спеціальності)
освітньо-професійної програми _____ «Право» _____
(найменування освітньої програми)

тип дисципліни вибіркова дисципліна, професійної та практичної підготовки

2019 рік

ПОГОДЖЕНО:

Гарант освітньої програми


(підпис) Є.О. Гіда
(прізвище, ініціали)

РЕКОМЕНДОВАНО:

Кафедрою фінансів, обліку та
фундаментальних економічних дисциплін
протокол № 1 від «03» вересня 2019 року

Завідувач кафедри


(підпис) Т.М. Сугак
(прізвище, ініціали)

Розробники:

Антонова Олена Михайлівна кандидат економічних наук, доцент кафедри
фінансів, обліку та фундаментальних економічних дисциплін

1. Опис навчальної дисципліни

Мова навчання: *українська*

Статус дисципліни: *вибіркова дисципліна, професійної та практичної підготовки*

Передумови вивчення навчальної дисципліни: *«Економічна безпека підприємства»* для здобувачів вищої освіти є вибірковою дисципліною, яка забезпечує формування вмінь, передбачених освітньо-кваліфікаційною характеристикою. Дисципліна вивчається на основі базової загальнооекономічної та правової підготовки з таких дисциплін як «Економічна теорія», «Макроекономіка», «Мікроекономіка», «Економіка підприємства», «Менеджменту», «Господарське право» та набуття ними відповідних фахових компетенцій.

Дисципліна є підґрунтям для подальшого вивчення дисциплін, пов'язаних з галузевою специфікою кожної спеціальності та спеціалізації. Знання з даної дисципліни дозволять успішно вивчати такі дисципліни, як: «Фінансовий менеджмент», «Стратегічне управління».

Предметом вивчення навчальної дисципліни *«Економічна безпека підприємства»* є наукові основи безпеки підприємницької структури, принципи, методи захисту підприємства в умовах ризику та невизначеності, методичні положення щодо формування системи економічної безпеки підприємства, також комп'ютерні технології, що використовуються в області економіки, організації та планування діяльності підприємства та засоби захисту категоризованої економічної інформації.

Інформаційний обсяг навчальної дисципліни. На вивчення навчальної дисципліни відводиться 120 годин 4 кредитів ECTS

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни *«Економічна безпека підприємства»* є формування теоретичних знань та практичних навичок економіко-правового характеру щодо розвитку відносин між зацікавленими особами зовнішнього та внутрішнього середовищ в системі управління підприємством з метою підвищення рівня його економічної безпеки в ринковій економіці.

Основними **завданнями** навчальної дисципліни *«Економічна безпека підприємства»* є оволодіння здобувачами вищої освіти знаннями щодо особливостей діяльності та розвитку підприємств в умовах ризику та невизначеності зовнішнього середовища і навичками щодо забезпечення відповідного рівня економічної безпеки підприємства; одержання знань з основоположних принципів побудови та функціонування систем економічної безпеки; одержання знань про механізми забезпечення інформаційної та економічної безпеки, функціональні складові економічної інформації; підготовка студента до подальшого поглибленого вивчення спеціальних дисциплін; вироблення навичок самостійного вивчення різних категорій інформації та проведення їх порівняльного аналізу при забезпеченні її інформаційної та економічної безпеки.

3. Компетентності та заплановані результати навчання

Дисципліна *«Економічна безпека підприємства»* забезпечує набуття здобувачами вищої освіти **компетентностей**:

Інтегральна компетентність:

Здатність аналізувати фінансову і монетарну політику та обґрунтовувати напрями їх удосконалення.

Здатність використовувати теоретичний та методичний інструментарій для діагностики і моделювання фінансової діяльності суб'єктів господарювання.

Здатність до пошуку, використання та інтерпретації інформації для вирішення професійних і наукових завдань в сфері фінансів, банківської справи та страхування.

Здатність розробляти завдання для проектування інформаційних систем в сфері фінансів, банківської справи та страхування.

Вміти обґрунтовувати напрями удосконалення фінансової і монетарної політики.

Здійснювати діагностику і моделювання фінансової діяльності суб'єктів господарювання.

Систематизувати та аналізувати інформацію для вирішення професійних та наукових завдань в сфері фінансів, банківської справи та страхування.

Розробляти завдання для проектування інформаційних систем в сфері фінансів, банківської справи та страхування

Загальні компетентності:

- здатність прогнозувати й критично оцінювати можливі напрями розвитку підприємства в умовах ризику та невизначеності стану зовнішнього середовища;
- вміння розробляти стратегічні плани розвитку підприємства з урахуванням небезпек та загроз його діяльності;
- здатність визначати тактичні та оперативні плани господарської діяльності підприємства через забезпечення відповідного рівня його економічної безпеки;
- спроможність передбачати напрями розвитку зовнішнього середовища та пов'язані з цим загрози діяльності підприємства;
- здатність передбачати й запобігати економічним ризикам; вміння розробляти плани підвищення економічної, соціальної та екологічної ефективності діяльності підприємства з урахуванням можливих ризиків.
- здатність створювати та забезпечувати здійснення конкретних програм розвитку підприємства з урахуванням ризику та невизначеності середовища господарювання;
- спроможність формувати та реалізовувати стратегію економічної безпеки підприємства в рамках загальної стратегії його розвитку;
- здатність організувати реалізацію стратегічних, тактичних, оперативних планів діяльності підприємства щодо забезпечення відповідного рівня його економічної безпеки;
- вміння формувати службу економічної безпеки на підприємстві; вміння розробляти положення про службу економічної безпеки; здатність розробляти функціональні обов'язки посадових осіб служби економічної безпеки;
- здатність організовувати ефективну конкурентну розвідку; вміння реалізовувати заходи щодо підвищення економічної, соціальної та екологічної ефективності діяльності підприємства з урахуванням можливих ризиків;
- здатність обґрунтовувати доцільність та забезпечувати ефективність взаємовідносин з відповідними зовнішніми організаціями щодо забезпечення економічної безпеки;
- вміння забезпечувати взаємодію служби економічної безпеки з керівництвом та іншими підрозділами підприємства.
- здатність забезпечувати зацікавленість персоналу у забезпеченні відповідного рівня економічної безпеки підприємства;
- вміння розробляти та впроваджувати заходи з мотивації персоналу підприємства з метою запобігання конфліктів та забезпечення їх узгодженої та плідної співпраці;
- спроможність володіти способами регуляції емоційної напруги в процесі ділового спілкування з питань забезпечення економічної безпеки підприємства;
- вміння використовувати неконфліктні підходи в процесі розроблення та прийняття колективних рішень щодо фінансово-господарської діяльності підприємства в умовах ризику та невизначеності.
- здатність виявляти порушення фінансової, кадрової, технічної дисципліни та розробляти й реалізовувати заходи з їх усунення;
- вміння контролювати виконання пропозицій щодо усунення виявлених недоліків, порушень і загроз економічній безпеці підприємства;
- вміння застосовувати та розробляти критерії оцінки ефективності діяльності служби економічної безпеки на підприємстві.
- здатність використовувати правила ефективного ділового спілкування щодо

управління економічною безпекою підприємства;

- здатність проводити колективні наради, переговори, узгоджувати інтереси всіх зацікавлених осіб щодо забезпечення відповідного рівня економічної безпеки підприємства;
- здатність впроваджувати заходи з профілактики конфліктних ситуацій у діяльності системи економічної безпеки;
- вміння вирішувати конфліктні ситуації в системі економічної безпеки підприємства.
- здатність організовувати інформаційне забезпечення прийняття рішення щодо доцільності ділової співпраці з урахуванням можливих ризиків;
- вміння забезпечувати встановлення ефективних контактів із потенційними діловими партнерами, формування та підготовку необхідних пакетів документів, угод, договорів з урахуванням можливих ризиків;
- спроможність реалізовувати заходи щодо забезпечення збереження довгострокових контактів із стратегічними діловими партнерами.
- вміння впроваджувати методiku та техніку гарантування безпеки на підприємствах всіх форм власності, різних видів діяльності;
- здатність визначати права та обов'язки відповідних підрозділів щодо забезпечення економічної безпеки діяльності підприємства;
- спроможність надавати рекомендації щодо усунення негативних факторів в роботі підрозділів підприємства.
- вміння збирати та обробляти первинну інформацію, яка використовується під час прийняття управлінських рішень;
- здатність володіти методами та засобами прийняття управлінських рішень в системі економічної безпеки підприємства;
- спроможність ініціювати дослідження і критичний аналіз чинників зовнішнього та внутрішнього середовищ господарювання підприємства; вміння формувати вимоги до розкриття інформації на підприємстві; здатність налагоджувати ефективну інформаційно-комунікаційну взаємодію між службою безпеки, іншими підрозділами, керівництвом підприємства та зовнішнім середовищем в умовах жорсткої конкуренції, прояву загроз, небезпек, ризику і конфліктів.
- спроможність здійснювати збір, оброблення інформації та інтерпретацію результатів щодо фінансово-господарської діяльності підприємства в мовах високого ступеня ризику та невизначеності зовнішнього середовища;
- вміння здійснювати збір, оброблення інформації та інтерпретацію результатів щодо діяльності служби безпеки на підприємстві;
- здатність досліджувати потенційні та реальні загрози економічній безпеці підприємства та аналізувати причини їх виникнення;
- вміння розробляти документарне забезпечення заходів з організації та здійснення діяльності служби безпеки на підприємстві;
- здатність проводити опитування різних категорій респондентів щодо актуальних питань економічної безпеки на підприємстві;
- вміння розробляти науково обґрунтовані методи, методики, підходи щодо підвищення рівня економічної безпеки підприємства.
- спроможність забезпечувати об'єктивну оцінку власного освітньо-професійного потенціалу;
- здатність відстежувати й використовувати новітні наукові та технічні досягнення у сфері забезпечення економічної безпеки підприємства;
- вміння ефективно застосовувати організаційні форми підвищення кваліфікації працівників служби економічної безпеки;
- спроможність забезпечити зацікавленість працівників служби економічної безпеки у навчанні та підвищенні кваліфікації.
- здатність учитися; креативність, здатність до системного мислення; наполегливість у досягненні мети; турбота про якість виконуваної роботи.
- навички роботи з комп'ютером; дослідницькі навички.

Спеціальні (фахові, предметні):

- базові уявлення про економічну інформацію й інформаційний обмін між суб'єктами та об'єктами підприємства;
- базові уявлення про розвиток інформаційних технологій на сучасному етапі;
- сучасні уявлення про роль і розвиток мережних технологій у житті світового суспільства;
- здатність застосовувати основні методи аналізу й оцінки стану систем економічної та інформаційної безпеки;
- здатність до ділових комунікацій, навички роботи в команді.
- здатність використовувати знання в галузі математичної статистики для статистичної обробки експериментальних даних;
- здатність використовувати математичний апарат для практичного оцінювання характеристик систем економічної та інформаційної безпеки;
- знання й уміння в галузі теоретичних основ інформатики й практичного використання комп'ютерних технологій;
- здатність володіти професійними навичками роботи з комп'ютером, використовувати інформаційні технології для рішення експериментальних і практичних завдань на підприємстві.
- здатність планувати й реалізовувати заходи щодо підвищення рівня автоматизації підприємства в сфері економічної та інформаційної безпеки;
- здатність організовувати облік та аудит систем економічної та інформаційної безпеки відповідно до вимог безпеки інформаційного обміну;
- знання правових основ і законодавства України в галузі інформаційної та економічної безпеки.

У результаті вивчення навчальної дисципліни здобувач освіти повинен

знати:

- наукові основи безпеки підприємницької структури; сутність економічної безпеки підприємства та її функціональні складові;
- значущі загрози та небезпеки економічній безпеці підприємства на різних інституційних рівнях;
- принципи організації системи економічної безпеки підприємства. основні підходи до гарантування безпеки; функції менеджменту безпеки підприємництва; основні нормативно правові документи, що регламентують діяльність служби безпеки на підприємстві;
- критерії оцінки та методи оцінювання рівня економічної безпеки підприємства;
- сутність, завдання та функції ділової розвідки, її основні напрями; способи захисту комерційної таємниці підприємства; засоби та методи забезпечення сталого економічного розвитку підприємства в сучасних умовах господарювання та їх ресурсне забезпечення;
- класифікацію систем економічної безпеки і основні принципи їх функціонування, призначення, типи і характеристики;
- моделі інформаційної та економічної безпеки, стандарти ББ та інші міжнародні й загальноприйняті стандарти відповідної галузі;
- особливості категорованої економічної інформації, що підлягає захисту та відповідні нормативні документи, які регламентують визначені категорії інформації;
- можливості програмного забезпечення для забезпечення інформаційної та економічної безпеки;
- методи оцінювання рентабельності використання необхідного програмного забезпечення інформаційної та економічної безпеки на підприємстві;
- основні загрози безпеки інформації і принципи створення комплексного захисту інформації;
- можливості ОС і спеціальних програм по забезпеченню безпеки категорованої економічної інформації.

вміти:

- Ставити завдання, аналізувати, давати порівняльну характеристику програмного забезпечення інформаційної та економічної безпеки на підприємстві.
- Розробляти вимоги щодо створення комплексу засобів та їх подальшого використання при забезпеченні інформаційної та економічної безпеки на підприємстві.
- Налагоджувати параметри програмного забезпечення, використовуючи можливості операційних систем з метою поліпшення рівня інформаційної та економічної безпеки.
- Вибирати, розробляти та використовувати засоби аудиту та діагностики систем економічної та інформаційної безпеки для підтримки їх надійного функціонування.
- Застосовувати математичні методи для моделювання наслідків втрати, пошкодження, зміни та інших несанкціонованих дій з економічною інформацією.
- Оформлювати прийняті управлінські рішення у вигляді комплексу документації, враховувати технологічні, ергономічні та естетичні фактори під час використання засобів забезпечення інформаційної та економічної безпеки.
- Оцінювати потенційні загрози безпеки економічної інформації і застосовувати засоби її захисту на усіх етапах виробничого циклу на підприємстві.
- Проводити об'єктивний аналіз ефективності прийнятих управлінських рішень, користуватися обраним технологічним апаратом щодо вирішення завдань підприємства, які виникають під час розробки та дослідження систем економічної та інформаційної безпеки.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Обсяг у годинах											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	сем.	пз	ла б.	с.р		л	сем.	пз	ла б.	с.р
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Організація економічної безпеки підприємства												
Тема 1. Поняття та основні категорії економічної безпеки	10	2	2	-	-	6	10	0,5	0,5	-	-	9
Тема 2. Індикатори та складові економічної безпеки підприємства	16	2	6	-	-	8	16	0,5	1,5	-	-	14
Тема 3. Системи економічної безпеки підприємства	14	2	4	-	-	8	14	0,5	1	-	-	12,5
Тема 4. Особливості діяльності служби безпеки підприємства	14	2	4	-	-	8	14	0,5	1	-	-	12,5
Тема 5. Недобросовісна конкуренція та захист комерційної таємниці	12	2	2	-	-	8	12	0,5	0,5	-	-	11
Тема 6. Ділова розвідка	9	1	2	-	-	6	9	0,25	0,5	-	-	8,25
Разом за змістовим модулем 1	75	11	20	-	-	44	75	2,75	5	-	-	67,25
Змістовий модуль 2. Основи інформаційної безпеки												
Тема 7. Загальні принципи безпеки інформаційних технологій	10	2	-	-	-	8	10	0,5	-	-	-	9,5
Тема 8. Канали витоку інформації	8	2	-	-	-	6	8	0,5	-	-	-	7,5
Тема 9. Організація інформаційної безпеки на підприємстві	10	2	-	-	-	8	10	0,5	-	-	-	9,5
Разом за змістовим модулем 2	28	6	-	-	-	22	28	1,5	-	-	-	26,5
Змістовий модуль 3. Особливості застосування ІБ у бізнесі												
Тема 10. Організація інформаційної безпеки комп'ютерної мережі	10	2	-	-	-	8	10	0,5	-	-	-	9,5
Тема 11. Правові основи інформаційної безпеки	7	1	-	-	-	6	7	0,25	-	-	-	6,75
Разом за змістовим модулем 3	17	3	-	-	-	14	17	0,75	-	-	-	16,25
Усього годин	120	20	20	-	-	80	120	5	5			110

5. Зміст програми навчальної дисципліни

Змістовий модуль 1. Організація економічної безпеки підприємства

Тема 1. Поняття та основні категорії економічної безпеки

Поняття економічної безпеки. Класифікація видів економічної безпеки зовнішнього та внутрішнього середовища системи. Сутність продовольчої, технологічної та соціальної безпеки на національному рівні. Проблеми співвідношення економічної безпеки особистості, підприємства, регіону та держави. Стан безпеки організації. Безпека як функція організації. Джерела негативних впливів на економічну безпеку підприємства. Основна мета економічної безпеки підприємства. Основні функціональні цілі економічної безпеки. Види заходів безпеки: загальні та спеціальні. Економічна безпека підприємства на різних стадіях життєвого циклу. Проблеми сучасного ринку, які обумовлюють необхідність економічно безпечного функціонування підприємства.

Об'єкт та предмет економічної безпеки. Групи суб'єктів економічної безпеки.

Чинники, що формують відповідний рівень економічної безпеки: безпосередні чинники виробництва, стабільний попит на продукцію, надійність постачальників, зовнішня конкуренція, державне економічне регулювання діяльності підприємства, надійний захист комерційної таємниці, компетентність керівництва підприємства.

Види загроз економічній безпеці за місцем, природою, ймовірністю, сферами виникнення, за наслідками, за відношенням до людської діяльності, за об'єктами посягань, за можливістю прогнозування. Економічні загрози. Фізичні загрози. Психологічно-інформаційні загрози. Ризики як фактори загроз економічній безпеці підприємства. Зовнішні та внутрішні джерела загроз: кримінальні структури, промислове шпигунство, фірми-розвідники, конкуренти, корумповані представники органів влади, правоохоронних органів, контролюючих органів, засобів масової інформації, керівники організації, менеджери середньої ланки, працівники підприємства, працівники служби безпеки.

Тема 2. Індикатори та складові економічної безпеки підприємства

Структура економічної безпеки підприємства. Внутрішньовиробничі (фінансова, кадрова, технологічна, правова, інформаційна, екологічна, силова) та позавиробничі (ринкова та інтерфейсна) складові економічної безпеки. Поняття індикаторів економічної безпеки підприємства.

Фінансова складова як внутрішньовиробнича функціональна складова економічної безпеки. Свідчення про послаблення фінансової складової. Типова послідовність дій щодо забезпечення фінансової складової економічної безпеки. Показники фінансової складової економічної безпеки. Області фінансової стійкості.

Безпека підприємства в інтелектуальній та кадровій сферах. Характеристика інтелектуальної складової. Особливості кадрової складової. Внутрішні та зовнішні загрози порушення інтелектуальної та кадрової складових економічної безпеки підприємства. Послідовність заходів щодо забезпечення інтелектуальної та кадрової складової. Показники інтелектуальної та кадрової складової. Кадри як внутрішня загроза безпеці підприємства. Зловживання з боку персоналу: дрібні разові розкрадання, систематичні розкрадання, «внутрішнє підприємництво». Функції та завдання кадрової служби в сфері забезпечення економічної безпеки.

Техніко-технологічна складова економічної безпеки підприємства. Загрози послаблення техніко-технологічної безпеки підприємства. Етапи забезпечення техніко-технологічна складова економічної безпеки. Показники техніко-технологічної складової економічної безпеки підприємства.

Політико-правова безпека підприємства. Основні причини виникнення внутрішніх і зовнішніх негативних впливів на політико-правову безпеку. Особливості процесу забезпечення політико-правової складової економічної безпеки. Індикатори оцінки рівня політико-правової безпеки підприємства.

Інформаційна складова безпеки. Показники інформаційної складової. Рівні інформаційної безпеки. Побудова системи інформаційної безпеки. Оцінювання інформаційних ризиків.

Безпека підприємства в екологічній сфері. Алгоритм процесу забезпечення екологічної складової економічної безпеки. Показники безпеки підприємства в екологічній сфері. Рівні екологічної безпеки.

Силова безпека підприємства. Негативні дії щодо силової складової. Показники силової безпеки підприємства. Послідовність дій щодо організації силової складової економічної безпеки.

Ринкова складова економічної безпеки підприємства. Свідчення ослаблення ринкової безпеки. Показники безпеки підприємства на ринку. Організація служби маркетингу як відповідального підрозділу за забезпечення ринкової складової.

Інтерфейсна складова економічної безпеки підприємства. Умови взаємодії з економічними контрагентами. Роль служби маркетингу в забезпеченні інтерфейсної складової.

Тема 3. Система економічної безпеки підприємства

Поняття та основні елементи системи економічної безпеки підприємства. Організація системи безпеки підприємства. Завдання, що вирішуються системою гарантування безпеки. Політика безпеки підприємства: поняття, цілі та складові. Програма гарантування безпеки підприємства. Особливості стратегічного управління в сфері безпеки. Тактика гарантування безпеки. Засоби гарантування безпеки: технічні, організаційні, фінансові, інформаційні, правові, кадрові, інтелектуальні. Механізм реалізації безпеки. Функції системи безпеки. Принципи забезпечення економічної безпеки. Режим функціонування системи економічної безпеки.

Концепція безпеки підприємства. Вимоги, що висуваються до концепції безпеки підприємства. Структура концепції економічної безпеки підприємства: опис проблемної ситуації в сфері безпеки підприємства, механізм гарантування безпеки, заходи щодо реалізації заходів безпеки.

Тема 4. Особливості діяльності служби безпеки підприємства

Служба безпеки як підсистема підприємства. Мета та завдання служби безпеки. Типові функції служби безпеки підприємства. Процедура створення та ліквідації служби безпеки підприємства. Кадрове, матеріально-технічне та правове забезпечення діяльності служби безпеки підприємства.

Структура та особливості управління діяльністю служби безпеки підприємства. Особливості підбору персоналу для роботи у службі безпеки. Складові служби безпеки підприємства: сектор охорони, режиму, технічного захисту, оперативної роботи. Завдання служби безпеки щодо гарантування режиму та охорони. Перевірка роботи служби безпеки. Особливості використання послуг зовнішніх охоронних організацій як альтернатива створення служби безпеки підприємства.

Тема 5. Недобросовісна конкуренція та захист комерційної таємниці

Комерційна таємниця підприємства. Відомості, що становлять комерційну таємницю підприємства. Правові аспекти комерційної таємниці.

Механізм визначення переліку інформації, що становить комерційну таємницю. Досвід іноземних підприємств щодо визначення комерційної таємниці. Тотальний, плагіаторський, аналітичний та експертний способи визначення комерційної таємниці.

Поняття та особливості недобросовісної конкуренції. Види недобросовісної конкуренції. Форми недобросовісної конкуренції: економічне, пряме фізичне придушення, промислове шпигунство.

Економічне шпигунство: поняття та особливості. Форми та методи економічного шпигунства. Шпигунство як спосіб добування інформації, що становить комерційну таємницю.

Налагодження охорони комерційної таємниці на підприємстві. Контроль персоналу. Використання технічних засобів.

Тема 6. Ділова розвідка

Поняття ділової розвідки. Історія виникнення та напрями розвитку ділової розвідки. Специфіка трактування ділової розвідки та її відмінність від промислового шпигунства.

Особливості ділової розвідки. Класифікація ділової розвідки за предметом інтересів. Перелік запитань, від яких залежить якість розвідки. Послідовність вирішення певних завдань ділової розвідки. Механізм діяльності ділової розвідки.

Роль ділової розвідки у бізнесі. Основні переваги компанії, що має сильну структуру ділової розвідки.

Змістовий модуль 2. Основи інформаційної безпеки

Тема 7. Загальні принципи безпеки інформаційних технологій

Поняття інформації та її захисту. Основні поняття захисту інформації: речова,

телекомунікаційна та документована. Інформаційні ресурси й процеси. Категорії інформації: державна таємниця, комерційна, службова та банківська тайна, персональна інформація.

Основні характеристики інформації: конфіденційність, цілісність та доступність. Методи порушення конфіденційності, цілісності й доступності інформації.

Загрози ІБ, їх класифікація та основні характеристики. Уразливість інформації. Основні групи загроз: порушення цілісності, порушення конфіденційності та доступності інформації. Аналіз погроз ІБ, проблеми інформаційної війни.

Існуючі стандарти ІБ, їх основні положення щодо використання в інформаційних технологіях. Нормативні документи на підприємстві для організації безпеки економічної інформації. Основні заходи щодо організації спеціального діловодства з носіями інформації.

Роботи, які пов'язані із розробкою й аналізом засобів забезпечення ІБ систем економічної та інформаційної безпеки на основі розроблених програм і методик, у тому числі із забезпеченням вимог, що випливають із документів, що регламентують режим безпеки даних.

Аналіз існуючих методів і засобів, застосовуваних для аудиту й захисту комерційної інформації, і розробка пропозицій по їхньому вдосконаленню й підвищенню ефективності.

Оцінка техніко-економічного рівня й ефективності запропонованих і реалізованих організаційно-технічних рішень, пов'язаних із застосуванням програмно-технічних засобів ІБ, з урахуванням перспектив і напрямків їхнього вдосконалення.

Тема 8. Канали витоку інформації

Історичний аспект виникнення та використання каналів витоку інформації.

Поняття каналу витоку інформації. Класифікація каналів витоку інформації, їх характеристики. Області використання каналів витоку інформації. Методи та засоби захисту каналів витоку інформації.

Поняття інформаційного потоку в каналі витоку інформації. Математичний опис інформаційного потоку.

Способи використання каналів витоку інформації у процесі діяльності підприємства.

Таємні канали витоку інформації. Організація виявлення таємних каналів витоку інформації. Моделі таємних каналів витоку інформації. Організація захисту інформації при визначенні таємних каналів витоку інформації.

Загальні класифікація віддалених мережних атак при використанні електронних каналів витоку інформації. Типові віддалені атаки. Атаки на основі використання стеку протоколів TCP/IP.

Основи використання сканерів ІБ в різних каналах витоку інформації. Властивості, достоїнства та недоліки використання сканерів ІБ. Аналіз інформації, отриманої при використанні сканерів ІБ.

Організація проведення різних видів аудиту інформації в різних каналах витоку інформації. Аналіз та подальше використання інформації, отриманої при проведенні аудиту. Формування «динаміки» використання каналів витоку інформації з метою отримання оцінки їх ефективності.

Тема 9. Організація інформаційної безпеки на підприємстві

Поняття політики безпеки (ПБ) на підприємстві. Приклади розроблених ПБ на підприємстві. Служби ІБ на підприємстві. Типові функціональні обов'язки співробітників служби ІБ. Методика розробки ПБ на підприємстві. Основні етапи реалізації ПБ в умовах сучасного бізнесу. Приклади сценаріїв злому ІС на підприємстві.

Багаторівнева структура ПБ. Математичний опис багаторівневої ПБ. Політика захисту цілісності Байба.

Типова структура підсистеми безпеки ОС і функції, які виконуються: ідентифікація й аутентифікація, розмежування доступу, аудит, підзвітність дій, повторне використання об'єктів, точність і надійність обслуговування, захист обміну даних. Реалізація підсистеми ІБ на підприємстві.

Відомі міжнародні стандарти управління ІБ: BS 7799 (ISO/IEC 17799 и ISO/IEC 27001), Orange Book, X.800, критерії Європейських держав, Control Objectives for Information and Related Technology (COBIT), IT Infrastructure Library (ITIL) и Statement on Auditing Standards (SAS) No. 70.

Архітектура систем попередження вторгнення – Intrusion Prevention Systems (IPS).

Організація конфігурування IPS для подальшого використання на підприємстві.

Архітектура систем визначення вторгнення – Intrusion Detection Systems (IDS). Організація конфігурування IDS для подальшого використання на підприємстві. Організація використання обох систем – IPS та IDS для забезпечення комплексного захисту.

Організація оптимального використання парольного захисту інформації на підприємстві. Властивості, достоїнства та недоліки використання парольного захисту. Розрахунок стійкості парольного захисту інформації. Використання парольного захисту інформації в різних системах.

Організація на підприємстві групи улагоджування інцидентів комп'ютерної безпеки (ГУІКБ). Її права, статус, обов'язки. Порядок й організація проведення розслідування за фактом комп'ютерного інциденту.

Системи автентифікації та ідентифікації. Класифікація систем автентифікації та ідентифікації. Особливості електронних систем автентифікації та ідентифікації.

Змістовий модуль 3. Особливості застосування ІБ у бізнесі

Тема 10. Організація інформаційної безпеки комп'ютерних мереж

Програмно-апаратні засоби забезпечення ІБ в комп'ютерних мережах. Протоколи автентифікації при вилученому доступі. Засоби й методи забезпечення цілісності й конфіденційності. Захист серверів і робочих станцій. Засоби захисту локальних мереж при підключенні до Інтернет. Захисні екрани. Захист віртуальних локальних мереж.

Організація ІБ мережі за допомогою брандмауерів та файєрволів. Проектування правил брандмауерів. Апаратні реалізації брандмауерів та файєрволів.

ІБ при роботі в мережі Інтернет. Типи ресурсів та сервісів в мережі Інтернет, які використовуються на підприємствах. ІБ при роботі із електронної поштою. Організація ІБ від несанкціонованого доступу при роботі із ресурсами ICQ, IRC, CHAT. Організація ІБ робочого місця працівника підприємства при роботі в мережі Інтернет. Використання програмних засобів запобігання несанкціонованого доступу.

Тема 11. Правові основи ІБ

Законодавство України в області ІБ, захисту державної таємниці й конфіденційної інформації. Види інформації, що захищається. Державна таємниця як особливий вид інформації, що захищається. Конфіденційна інформація. Система захисту державної таємниці. Правовий режим захисту державної таємниці. Ліцензійна й сертифікаційна діяльності в області ІБ. Правові основи захисту інформації із використанням застосування технічних засобів (захисту від технічних розвідок, застосування й розробка шифрувальних засобів і т.д.). Захист інтелектуальної власності засобами патентного й авторського права. Правова регламентація охоронної діяльності. Міжнародне законодавство в області ІБ. Злочини в сфері комп'ютерної інформації. Експертиза злочинів в області комп'ютерної інформації. Криміналістичні аспекти проведення розслідувань.

Наслідки порушення ІБ на підприємстві. Основні закони та положення України, які регламентують відповідальність за порушення ІБ.

Правовий статус ГУІКБ на підприємстві. Юридичний аспект функціонування ГУІКБ на підприємстві. Відповідальність членів ГУІКБ.

Підсумковий модульний контроль

Екзамен

6. Теми лекцій

№ з/п	Назва теми	Обсяг у годинах	
		Денна форма	Заочна форма
1	Поняття та основні категорії економічної безпеки	2	0,5
2	Індикатори та складові економічної безпеки підприємства	2	0,5
3	Система економічної безпеки підприємства	2	0,5
4	Особливості діяльності служби безпеки підприємства	2	0,5
5	Недобросовісна конкуренція та захист комерційної таємниці	2	0,5
6	Ділова розвідка	1	0,25
7	Загальні принципи безпеки інформаційних технологій	2	0,5
8	Канали витоку інформації	2	0,5
9	Організація інформаційної безпеки на підприємстві	2	0,5
10	Організація інформаційної безпеки комп'ютерних мереж	2	0,5
11	Правові основи ІБ	1	0,25
Усього годин		20	5

7. Теми практичних занять

№ з/п	Назва теми	Обсяг у годинах	
		Денна форма	Заочна форма
1	Не передбачено	-	-
Усього годин		-	-

8. Теми семінарських занять

№ з/п	Назва теми	Обсяг у годинах	
		Денна форма	Заочна форма
1	Поняття та основні категорії економічної безпеки	2	0,5
2	Індикатори та складові економічної безпеки підприємства	6	1,5
3	Системи економічної безпеки підприємства	4	1
4	Особливості діяльності служби безпеки підприємства	4	1
5	Недобросовісна конкуренція та захист комерційної таємниці	2	0,5
6	Ділова розвідка	2	0,5
Усього годин		20	5

ПЛАНІ СЕМІНАРСЬКИХ ЗАНЯТЬ З ДИСЦИПЛІНИ «ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВ»

Тема 1. Поняття та основні категорії економічної безпеки

1. Ризики як фактори, що несуть загрози економічній безпеці розвитку підприємства.
2. Втрати в комерційному та виробничому підприємстві, ймовірність їх виникнення в українських умовах господарювання та заходи з їх усунення.
3. Послідовність етапів управління ризиками діяльності підприємства та їх взаємозв'язок з функціями управління.

Література: основна [2-10; 17]; додаткова [30; 32; 33; 35; 36; 39; 40].

Тема 2. Індикатори та складові економічної безпеки підприємства

1. Внутрішні та зовнішні ризики діяльності підприємства та їх вплив на стан функціональних складових економічної безпеки підприємства.
2. Індикатори економічної безпеки особистості, підприємства, регіону та держави, їх порогові значення та напрями зміни.
3. Особливості експертного оцінювання рівня економічної безпеки підприємства за її складовими.

Література: основна [2; 6; 8-10; 17]; додаткова [32; 34; 36; 40; 41].

Тема 3. Система економічної безпеки підприємства

1. Стійкість підприємства як важлива складова його економічної безпеки.
2. Адаптація підприємства та її види.
3. Організація інформаційного забезпечення адаптації підприємства.
4. Планування та бюджетування процесу адаптації.

Література: основна [2; 6-10; 17]; додаткова [31; 32; 36; 38; 40; 43].

Тема 4. Особливості діяльності служби безпеки підприємства

1. Ризики та загрози процесів взаємодії з контрагентами підприємства.
2. Інформаційно-психологічна безпека персоналу підприємства.
3. Управління мотивацією персоналу як фактор забезпечення економічної безпеки підприємства.
4. Інформаційна взаємодія служби безпеки з іншими підрозділами підприємства.

Література: основна [2-6; 8-10; 17]; додаткова [32; 36; 38; 40].

Тема 5. Недобросовісна конкуренція та захист комерційної таємниці

1. Обґрунтування складу осіб, яких доцільно залучити в групу з розробки положення про режим доступу до інформації підприємства.
2. Визначення складу відомостей, які слід віднести до категорії конфіденційної та таємної інформації (на прикладі підприємств різних видів економічної діяльності).

Література: основна [2; 6; 8-10; 17]; додаткова [32; 36; 40; 42].

Тема 6. Ділова розвідка

1. Визначення складу осіб, зацікавлених у діяльності підприємства та спроможних порушити його економічну безпеку, кола їх інформаційних потреб.
2. Визначення джерел інформації, якими можливо скористатися з метою порушення економічної безпеки підприємства.
3. Формування переліку економічних рішень, які можуть бути реалізовані різними суб'єктами в напрямі порушення економічної безпеки підприємства.

Література: основна [2; 3; 6; 8-10; 17]; додаткова [32; 36; 40].

9. Самостійна робота

№ з/п	Назва теми	Обсяг у годинах	
		Денна форма	Заочна форма
1	Поняття та основні категорії економічної безпеки	6	9
2	Індикатори та складові економічної безпеки підприємства	8	14
3	Система економічної безпеки підприємства	8	12,5
4	Особливості діяльності служби безпеки підприємства	8	12,5
5	Недобросовісна конкуренція та захист комерційної таємниці	8	11
6	Ділова розвідка	6	8,25
7	Загальні принципи безпеки інформаційних технологій	8	9,5
8	Канали витоку інформації	6	7,5
9	Організація інформаційної безпеки на підприємстві	8	9,5
10	Організація інформаційної безпеки комп'ютерних мереж	8	9,5
11	Правові основи ІБ	6	6,75
Усього годин		80	110

ПИТАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

Змістовний модуль 1. Організація економічної безпеки підприємства

Тема 1. Поняття та основні категорії економічної безпеки

1. Передумови виникнення поняття економічної безпеки підприємства та його еволюція.
2. Міжнародна економічна безпека як наслідок глобалізації.
3. Особливості забезпечення національної економічної безпеки.
4. Концепція забезпечення соціально-економічної безпеки регіону.

Література: основна [2-10; 17]; додаткова [30; 32; 33; 35; 36; 39].

Тема 2. Індикатори та складові економічної безпеки підприємства

1. Аналіз прибутковості підприємства.
2. Критерії економічної безпеки підприємства.
3. Оцінювання рівня економічної безпеки підприємства.

Література: основна [2; 6; 8-10; 17]; додаткова [32; 34; 36; 40; 41].

Тема 3. Система економічної безпеки підприємства

1. Система пріоритетних інтересів підприємства як основа механізму забезпечення його економічної безпеки.
2. Структура механізму забезпечення економічної безпеки підприємства.
3. Адаптація підприємства як спосіб забезпечення його економічної безпеки.
4. Державне регулювання діяльності підприємств у забезпеченні їх економічної безпеки.

Література: основна [6-8; 17]; додаткова [31; 32; 36; 38; 40; 41].

Тема 4. Особливості діяльності служби безпеки підприємства

1. Процедура створення та ліквідації служби безпеки підприємства.
2. Перевірка роботи служби безпеки.
3. Використання послуг державної служби охорони та зовнішніх охоронних підрозділів як альтернатива створення служби безпеки підприємства.

Література: основна [2-6; 8-10; 17]; додаткова [32; 36; 38; 40].

Тема 5. Недобросовісна конкуренція та захист комерційної таємниці

1. Поняття та особливості комерційної інформації підприємства.
2. Загрози інформаційній безпеці підприємства.
3. Напрями підвищення стійкості функціонування інформаційної системи підприємства.
4. Правові аспекти комерційної таємниці.

Література: основна [2-6; 8-10; 17]; додаткова [32; 36; 40; 42].

Тема 6. Ділова розвідка

1. Історія виникнення ділової розвідки.
2. Стратегія безпечного розвитку підприємства в умовах інформаційної війни.

Література: основна [1-3; 6; 8-10; 17]; додаткова [32; 36; 40].

Змістовний модуль 2. Основи інформаційної безпеки

Тема 7. Загальні принципи безпеки інформаційних технологій

1. Дайте визначення інформації, її категорії.
2. Визначте мету використання державної інформаційної політики.
3. У чому полягають принципові відмінності різних категорій інформації.
4. Що дозволяє виявити використання існуючих стандартів ІБ.
5. Назвіть основні принципи побудови ІБ.
6. Назвіть основні загрози ІБ.
7. Дайте визначення національної безпеки.
8. Опишіть загальнометодологічні принципи теорії ІБ.

Література: основна [1; 2; 17]; додаткова [26; 28; 30; 32-34].

Тема 8. Канали витоку інформації

1. Опишіть історію виникнення та використання каналів витоку інформації.
2. Визначте поняття каналу витоку інформації та їх класифікацію.
3. У чому полягають принципові відмінності різних каналів витоку інформації.
4. Опишіть основні характеристики таємних каналів витоку інформації.
5. Основні характеристики сканерів ІБ.
6. Методика проведення різних видів аудиту інформації в різних каналах витоку інформації.

Література: основна [1; 17]; додаткова [30; 34; 35].

Тема 9. Організація інформаційної безпеки на підприємстві

1. Визначте мету використання ІБ на підприємстві.
2. Опишіть процес розробки ІБ на підприємстві.
3. Дайте визначення політики захисту цілісності Байба.
4. У чому полягають принципові відмінності міжнародних стандартів управління ІБ.
5. Області використання систем попередження вторгнення.

6. Назвіть основні принципи побудови систем визначення вторгнення.
7. Приведіть класифікацію систем автентифікації та ідентифікації.

Література: основна [1; 2; 3; 17]; додаткова [27; 28; 31; 33; 36; 37].

Змістовний модуль 3. Особливості застосування ІБ у бізнесі

Тема 10. Організація інформаційної безпеки комп'ютерних мереж

1. Дайте визначення протоколу автентифікації при вилученому доступі.
2. Дайте визначення цілісності й конфіденційності.
3. Дайте визначення вразливості.
4. Класифікуйте основні типи брандмауерів та файрволів.
5. У чому полягають принципи захисту віртуальних локальних мереж.
6. Области використання програмних засобів запобігання несанкціонованого доступу.
7. Назвіть основні принципи побудови технології захисту мережі – IPSec.

Література: основна [2; 3; 17]; додаткова [28; 31; 32; 34; 36].

Тема 11. Правові основи ІБ

1. Дайте визначення видів інформації, що належать для захисту.
2. Дайте визначення державної таємниці.
3. У чому полягають принципові відмінності ліцензійної й сертифікаційної діяльності в області ІБ.
4. Области використання патентного й авторського права.
5. Основні закони та положення України, які регламентують відповідальність за порушення ІБ.
6. Юридичний аспект функціонування ГУІКБ на підприємстві.

Література: основна [1; 3; 17]; додаткова [28; 32; 34; 35].

КОНТРОЛЬНІ ЗАПИТАННЯ ДО ІСПИТУ

Змістовний модуль 1. Організація економічної безпеки підприємства

1. Що таке економічна безпека?
2. У чому полягає сутність економічної небезпеки?
3. Який зв'язок можна визначити між економічною небезпекою та економічним правопорушенням?
4. Які є види заходів безпеки?
5. Що таке загрози економічній безпеці?
6. Які є види загроз?
7. Що таке економічна загроза і чим вона відрізняється від економічної небезпеки?
8. Що таке фізичні загрози?
9. Що таке психологічно-інформаційні загрози?
10. Які є джерела загроз?
11. Які економічні загрози та небезпеки існують для підприємства на світовому, національному та індивідуальному рівні?
12. Що таке індикатори економічної безпеки підприємства?
13. Які існують критерії визначення економічної безпеки на макро-, мезо- та мікроекономічному рівнях господарювання, а також на рівні окремої особистості?
14. Які є джерела негативних впливів на економічну безпеку підприємства?
15. Які основні функціональні цілі економічної безпеки?
16. Якою є структура економічної безпеки підприємства?
17. Якими є показники безпеки підприємства у фінансовій сфері?
18. Якими є показники безпеки підприємства у кадровій сфері?
19. Якими є показники безпеки підприємства в інформаційній сфері?
20. Якими є показники безпеки підприємства у силовій сфері?
21. Якими є показники безпеки підприємства у ринковій сфері?

22. Якими є показники безпеки підприємства в інтерфейсній сфері?
23. Якими є показники безпеки підприємства в екологічній сфері?
24. Які існують методичні підходи до оцінювання економічної безпеки підприємства?
25. Що таке система безпеки організації?
26. Яка основна мета системи безпеки?
27. Які основні завдання системи безпеки?
28. Які об'єкти та суб'єкти безпеки?
29. Що є предметом економічної безпеки підприємства?
30. Яким є механізм реалізації безпеки?
31. Які основні функції системи безпеки?
32. Які основні засоби економічної безпеки?
33. Які є режими функціонування системи економічної безпеки?
34. Що таке концепція безпеки підприємства?
35. Яким є алгоритм побудови системи економічної безпеки підприємства?
36. У чому полягає сутність процесу адаптації та формування її бюджету?
37. У чому полягає взаємозв'язок ознак стійкості та адаптивності безпечного стану системи?
38. Чим визначається ефективність системи безпеки підприємства?
39. Які принципи гарантування економічної безпеки?
40. Що таке служба безпеки підприємства?
41. Якими є функції діяльності служби безпеки?
42. Який порядок створення служби безпеки?
43. Який порядок ліквідації служби безпеки?
44. Які ресурси необхідні для ефективної діяльності служби безпеки?
45. Як здійснюється відбір працівників в службу безпеки?
46. Що таке програма забезпечення безпеки підприємства?
47. Які особливості взаємодії служби безпеки на підприємстві з іншими підрозділами та суб'єктами зовнішнього середовища?
48. Які дії служби безпеки можливі у кризовій ситуації?
49. Які заходи загальної безпеки на підприємстві?
50. Які існують заходи протидії рекету?
51. Що таке керівництво службою безпеки підприємства і хто його здійснює?
52. Якими є повноваження начальника служби безпеки підприємства?
53. Якими є основні завдання служби режиму та охорони?
54. У чому сутність та значення комерційної інформації?
55. Що належить до категорії ділової інформації?
56. Як виявляються втрати підприємства через недотримання умов конфіденційності?
57. Що таке комерційна таємниця?
58. Яким є механізм визначення переліку інформації, що становить комерційну таємницю?
59. Якими є методи викрадення таємниць підприємства?
60. Чим державна таємниця відрізняється від комерційної?
61. Що таке недобросовісна конкуренція?
62. Які є форми недобросовісної конкуренції?
63. Які є способи незаконного добування інформації?
64. Що розуміється під незаконним використанням відомостей, які становлять комерційну таємницю?
65. Як визначаються втрати підприємства від порушення комерційної таємниці?

66. Які є форми і методи економічного шпигунства?
67. У чому суть та особливості ділової розвідки?
68. Які існують внутрішні та зовнішні джерела інформації ділової розвідки?
69. Яким чином впливає науково-технічний прогрес на розвиток економічної розвідки?
70. У чому особливості історичного розвитку ділової розвідки?
71. Яка специфіка створення розвідувальних структур у системі безпеки підприємства?
72. У чому суть діяльності ділової розвідки?
73. За якими критеріями доцільно оцінювати джерела та зміст інформації, що отримала ділова розвідка?
74. Які можливі напрями перевірки ділового партнера?
75. Чим відрізняється ділова розвідка від промислового шпигунства?
76. Які основні переваги підприємства з сильною структурою ділової розвідки?
77. Яка роль ділової розвідки у безпеці бізнесу?

Змістовний модуль 2. Основи інформаційної безпеки

1. У чому полягають принципові відмінності категорій інформації.
2. Причини використання ПБ.
3. Назвіть основні принципи побудови теорії ІБ.
4. Назвіть типи загроз ІБ.
5. Назвіть існуючі стандарти ІБ.
6. Приведіть цілі створення комп'ютерних мереж.
7. Що таке комп'ютерна мережа?
8. Який пристрій вперше використовувався для забезпечення доступу до головного комп'ютера з терміналів, віддалених від нього на багато сотень і тисячі кілометрів?
9. В якому році була створена комп'ютерна мережа, яка стала відправною точкою для створення першої і найвідомішої нині глобальної мережі – Інтернет?
10. Що таке мережна технологія?
11. Які мережі відносяться до телекомунікаційних мереж?
12. Які критерії є підставою для класифікації мереж?
13. Які бувають мережі за ступенем географічного розповсюдження?
14. Яка мережа призначена для відносно невеликих за масштабом підприємств, офісів і т.п.?
15. Які бувають комп'ютерні мережі за призначенням?
16. До якого типу мереж відноситься мережа навчальної лабораторії?
17. У чому принципова різниця між доступом до ресурсів «На рівні ресурсів» і «На рівні користувача».
18. Перерахуйте перелік дозволів, які можна встановити для папки. Чи відрізняється він від переліку дозволів для файлів?
19. Які частини URL можна опускати при завданні адреси Web-сторінки?
20. Що таке пошукова машина?
21. Назвіть відомі вам пошукові сервери.
22. Що таке портал? Назвіть адреси URL відомих порталів.
23. Назвіть можливості і переваги електронної пошти.
24. Призначення і взаємодія серверів POP3, SMTP?
25. У яких форматах можуть відправлятися поштові повідомлення? За допомогою якої команди це встановлюється?
26. Назвіть адреси електронної пошти вашої організації, вашого провайдера, вашого комп'ютера в локальній мережі.
27. Для чого служить доменне ім'я?

28. За якою схемою здійснюється перетворення адреси?
29. Для чого застосовується команда ping ya.ru?
30. Якими критеріями характеризується мережа?
31. Що таке ідеальна мережа?
32. Чим характеризується продуктивність мереж?
33. Що дозволяє виявити використання каналів витоку інформації.
34. Назвіть основні принципи побудови каналів витоку інформації.
35. Назвіть типи таємних каналів витоку інформації.
36. Назвіть основні принципи побудови ліцензійної й сертифікаційної діяльності в області ІБ.
37. Назвіть закони та положення України, які регламентують відповідальність за порушення ІБ.
38. Назвіть області використання патентного й авторського права.
39. Назвіть переваги ГУІКБ на підприємстві.
40. Назвіть типи брендмауерів та файерволів.
41. Яку кримінальну відповідальність визначають закони України за комп'ютерні злочини?
42. Що таке цифровий підпис?
43. Назвіть закони України, що визначають статус електронного підпису.
44. Дайте визначення ПБ.
45. Дайте визначення систем попередження вторгнення.
46. У чому полягають принципові відмінності систем визначення вторгнення.
47. Области використання систем автентифікації та ідентифікації.
48. Назвіть основні принципи міжнародних стандартів управління ІБ.
49. Назвіть типи устаткування, використовувані в ПБ.
50. Чому виникла необхідність у захисті комп'ютерів?
51. Що таке інформаційна безпека?
52. Що таке захист інформації?
53. Чому безпека – це процес, а не кінцевий результат?
54. На яких категоріях базується інформаційна безпека?
55. Перерахуйте критерії, за якими можна класифікувати загрози інформації?
56. Що відноситься до шкідливого програмного забезпечення?
57. Які методи захисту інформації ви знаєте?
58. Що таке ідентифікація?
59. Що таке автентифікація користувача?
60. Яким чином здійснюється автентифікація користувача?
61. Які три речі можуть використовуватися для встановлення достовірності особи?
62. Назвіть два типи біометричних систем.
63. Які методи захисту інформації відносяться до формальних засобів?
64. Чим відрізняються методи спонування від методів примушення. Приведіть приклади засобів, які реалізують ці методи.
65. Чому фізичний захист не може гарантувати безпеку?
66. Що таке електронний документ?
67. Для чого і як здійснюється сертифікація часу?
68. Назвіть основні помилки при виборі паролів.
69. Чому для розшифрування повідомлень, зашифрованих методом перестановки, марно застосовувати частотний аналіз для злому?
70. Приведіть приклад шифрування по методу перемножування матриць.

71. Назвіть найефективніший метод захисту інформації в бездротових мережах.

Змістовний модуль 3. Особливості застосування ІБ у бізнесі

1. Назвіть типи протоколів автентифікації.
2. Дайте визначення брандмауера.
3. Дайте визначення файрвола.
4. У чому полягають принципи відмінності брандмауерів та файрволів.
5. Області використання технології захисту мережі – IPSec.
6. Назвіть основні принципи побудови програмних засобів запобігання несанкціонованого доступу.
7. Назвіть типи брандмауерів та файрволів.
8. Назвіть основні принципи побудови ліцензійної й сертифікаційної діяльності в області ІБ.
9. Назвіть закони та положення України, які регламентують відповідальність за порушення ІБ.
10. Назвіть області використання патентного й авторського права.
11. Назвіть переваги ГУІКБ на підприємстві.

10.Індивідуальні завдання

Підготувати доповідь з дослідження конкретної організації з використанням блок-схем, за наступними розділами:

Оцінити рівень економічної безпеки підприємства на основі показників стану економічної і фінансової безпеки підприємства.

Визначити основні загрози економічної безпеки для підприємства.

Сформувати можливу стратегію підвищення рівня економічної безпеки підприємства.

Для закріплення теоретичних знань і практичних навичок з дисципліни здобувачі вищої освіти зобов'язані протягом семестру виконати і до початку екзаменаційної сесії індивідуальну контрольну роботу.

Контрольне завдання видається індивідуально кожному здобувачу вищої освіти з метою перевірити засвоєння теоретичної частини навчальної дисципліни та набуття практичних навичок у вирішенні поставлених задач.

Завдання на контрольну роботу видаються здобувачам вищої освіти відразу ж після прочитання настановних лекцій з дисципліни.

Виконується завдання на аркушах формату А4 на комп'ютері або рукописно з дотриманням вимог нормоконтролю до оформлення матеріалу.

Вимоги нормоконтролю до оформлення матеріалу: робота повинна бути виконана технічно і літературно грамотно: надрукована (або написана) на одній стороні аркуша формату А4; за рукописним способом пояснювальну записку виконують з розрахунку 30-35 рядків на сторінці, за машинним способом шрифтом 14 з міжрядковим інтервалом 1,5; текст слід писати, дотримуючись наступних розмірів полів: лівий – 30 мм, верхній та нижній – 20 мм, правий – 10 мм; всі лінії, букви, цифри і знаки повинні бути одного кольору (чорного, фіолетового або синього) абзацний відступ повинен бути однаковим упродовж усього тексту пояснювальної записки і дорівнювати п'яти знакам; сторінки нумерують арабськими цифрами і проставляють в правому верхньому кутку; ілюстрації і таблиці слід розташовувати в роботі безпосередньо після тексту, в якому вони згадуються вперше, або на наступній сторінці; назва таблиці або рисунка повинна бути короткою і відображати його зміст, і пишеться з великої букви. В кінці назви таблиці або рисунка крапка не ставиться.

Титульний аркуш включається в загальну нумерацію сторінок записки але номер сторінки не проставляється.

При виконанні практичного завдання варто дотримуватися наступних вимог: перед рішенням завдання необхідно навести його умову; рішення завдання варто супроводжувати необхідними формулами, розрахунками, короткими поясненнями; всі розрахунки показників

виконуються з точністю від 0,01, до 0,1%; наприкінці роботи вказується перелік використаної літератури, ставиться підпис здобувача вищої освіти та дата.

11. Критерії та порядок оцінювання результатів навчання

Контроль знань здобувачів вищої освіти

Контроль та оцінювання теоретичних знань та практичних навичок здобувачів вищої освіти протягом вивчення дисципліни відбувається за результатами тестування, розв'язання розрахунково-аналітичних завдань, обговорення конкретних ситуацій, а також у процесі контролю самостійної роботи.

Робоча програма передбачає застосування трьох форм контролю знань здобувачів вищої освіти:

- *поточний контроль* проводиться за кожною темою шляхом тестування, перевірки індивідуальних та колективних завдань, обговорення конкретних ситуацій, перевірки завдань для самостійної роботи, кожне з яких оцінюється за відповідними критеріями у балах.
- *модульний контроль* проводиться за певним блоком тем шляхом тестування, виконання контрольної роботи.
- *підсумковий контроль*. Формою підсумкового контролю є екзамен.

Критерії оцінювання знань здобувачів вищої освіти

Для визначення ступеня засвоєння навчального матеріалу та поточного оцінювання знань здобувачів вищої освіти враховується їх наступне ранжиювання:

I рівень знань. Здобувач вищої освіти володіє усім обсягом навчального матеріалу на теоретично-репродуктивному рівні.

II рівень знань. Здобувач вищої освіти володіє повним обсягом навчального матеріалу, здатний його аналізувати, але не має достатніх знань для формування висновків, не завжди здатний асоціювати теоретичні знання з практичними прикладами.

III рівень знань. Здобувач вищої освіти вільно володіє навчальним матеріалом на підставі вивченої основної та додаткової літератури, аргументовано висловлює власні думки, проявляє творчий підхід до виконання індивідуальних та колективних завдань аудиторної і самостійної роботи.

Порядок переведення оцінок у систему ЄКТС

Сума балів за всі види навчальної діяльності	ОЦІНКА ECTS	ОЦІНКА ЗА НАЦІОНАЛЬНОЮ ШКАЛОЮ	
		для екзамену, курсового проекту (роботи), практики	для заліку
90-100	A	відмінно	зараховано
82-89	B	добре	
75-81	C		
64-74	D	задовільно	
60-63	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-34	F	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

12. Форми поточного та підсумкового контролю успішності навчання

У процесі вивчення дисципліни «Економічна безпека підприємства» викладачем використовуються поточний та підсумковий контроль знань (опитування, контрольні та індивідуальні завдання, тестування тощо), презентації, екзамен (усний або письмовий).

13.Методичне забезпечення

1. Робоча програма дисципліни.
2. Конспект лекцій дисципліни.
3. Комплекс навчально-методичного забезпечення дисципліни.

14.Рекомендована література

Основна

1. Баяндин Н.И. Технологии безопасности бизнеса: введение в конкурентную разведку: учебн.-практ. пособ. / Баяндин Н.И. – М.: Юрист, 2002. – 320 с.
2. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – К.: ООО «ТИД «ДС», 2001. – 688 с.
3. Варналій З.С., Живко З.Б., Білик Р.Р., Онищенко С.В., Живко М.О. Фінансова безпека: навч.посібник; за ред.З.С.Варналія. Львів: Ліга-Прес, 2018. 300 с.
4. Економічна безпека в Україні: держави, фірми, особи: навч. посібн./ Реверчук А.Й., Малик Я.Й., Кульчицький І.І. та ін. – Львів: ЛФМАУП, 2000. – 192 с.
5. Економічна безпека підприємств, організацій та установ: навч. посіб. / В.Л. Ортинський, І.С. Керницький, З.Б. Живко та ін. – К.: Правова єдність, 2009. – 544 с.
6. Жебка В.В., Антонова О.М. Урікова О.М. Фінансовий менеджмент: Навч. посіб. – 2-ге вид., випр. і доп. – К.: Логос, 2017. – 312 с. *(Навчальний посібник з грифом МОН України (лист № 1/11-2547 від 27.02.2012р.)*
7. Живко З.Б. Економічна безпека підприємства: сутність, механізми забезпечення, управління. Монографія / З.Б.Живко. – Львів: Ліга-Прес, 2012. – 256 с.
8. Живко З.Б. Методологія управління економічною безпекою підприємства. Монографія / З.Б.Живко. – Львів : Вид-во Ліга-Прес, 2013. – 474 с.
9. Зубок М.І. Безпека підприємницької діяльності: нормативно- правові документи комерційного підприємства, банку / Зубок М.І., Зубок Р.М. – К.: Істина, 2004. – 144 с.
10. Кавун С.В. Информационная безопасность в бизнесе: научное издание. – Х.: Вид. ХНЕУ, 2007. – 408 с.
11. Кавун С.В. Інформаційна безпека: навч. посіб. Ч. 1. / Кавун С.В., Носов В.В., Манжай О.В. – Х. Вид. ХНЕУ, 2008. - 352 с.
12. Кавун С.В. Інформаційна безпека: навч. посіб. Ч. 2. / Кавун С.В., Носов В.В., Манжай О.В. – Х.: Вид. ХНЕУ, 2008. – 196 с.
13. Кавун С.В. Інформаційна безпека: підручник / С.В. Кавун. – Х.: Вид. ХНЕУ, 2009. – 368 с.
14. Кавун С.В. Лабораторний практикум з навчальної дисципліни інформаційна безпека: навч.-практ. посібн. / Кавун С.В., Носов В.В., Огурцов В.В. та ін. – Х.: Вид. ХНЕУ, 2008. – 256 с.
15. Камлик М.І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект: навч. посібн. / Камлик М.І. – К.: Атіка, 2005. – 432 с.
16. Керницький І. С., Живко З. Б., Копитко М. І. Конкурентна розвідка підприємств: курс лекцій. Львів: Ліга-Прес, 2015. 388с.
17. Козаченко Г.В. Економічна безпека підприємства: сутність та механізм забезпечення: монографія / Козаченко Г.В., Пономарьов В.П., Ляшенко О.М. – К.: Лібра, 2003. - 280 с.
18. Куркин Н.В. Управление экономической безопасностью развития предприятия: монография / Куркин Н.В. – Днепропетровск: АРТ-ПРЕСС, 2004. – 284 с.
19. Низенко Е.И. Обеспечение безопасности предпринимательской деятельности: учебн. пособ. / Низенко Е.И. – К.: МАУП, 2003. – 124 с.
20. Олейников Е.А. Экономическая и национальная безопасность: учебник для вузов / Е.А. Олейников. – М.: Экзамен, 2005. – 766 с.
21. Основи економічної безпеки: підручник / Бандурка О.М., Духов В.Є., Петрова К.Я. та ін. – Х.: Вид. НУВС, 2003. – 236 с.
22. Петренко И.Н. Безопасность экономического пространства хозяйствующего субъекта / И.Н. Петренко. – М.: Анкил, 2005. – 280 с.
23. Пономаренко В.С. Концептуальні основи економічної безпеки: монографія / В. С.

Пономаренко, С.В. Кавун. – Х.: Вид. ХНЕУ, 2008. – 256 с.

24. Симонович С. В. INTERTET: Лабораторія майстра : практ. посібн. з ефективних прийомів роботи в Інтернеті / С.В. Симонович, Г.А. Євсєєв, В. І. Мураховський. – М.: АСТ-ПРЕСС; Инфорком-Пресс, 2000. – 720 с.

25. Экономическая безопасность / под ред. Е.Л. Олейникова. – М.: РЭА им. Плеханова, 2000. – 285 с.

26. Цимбалюк М.М., Керницький І.С., Живко З.Б., Копитко М.І. Конкурентна розвідка: курс лекцій. Львів: Ліга-Прес, 2013. 264 с.

Допоміжна

27. Агафонов Г.Г. Концепции безопасности / Агафонов Г.Г., Буришев С.А., Прохоров С.Л. – К.: А-ДЕПТ, 2005. – 270 с.

28. Антонова О.М. Формування фінансово-економічного механізму забезпечення економічної безпеки ВНЗ. Актуальні проблеми економіки. 2016. № 3. С. 117-125.

29. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи / О.А. Баранов. – К.: ВД «СофтПрес», 2005. – 316 с.

30. Бруксбенк Д. Руководство по безопасности / Бруксбенк Д., Уилсон Дж.; пер. с англ. – М.: ЮНИТИ-ДАНА, 2003. – 319 с.

31. Варналій З.С. Системні проблеми та шляхи забезпечення фінансової безпеки України в умовах гібридної війни / З.С. Варналій, Т.Т. Томашеський // Економічний вісник університету. Збірник наук. праць учених та аспірантів. Випуск 41, Переяслав-Хмельницький, 2019. С.171-179.

32. Варналій З.С. Використання теорії нечітких множин для оцінки рівня фінансової безпеки підприємства / З.С. Варналій, А.М. Мехед // Міжнародний науковий журнал «Інтернаука», Серія: «Економічні науки». – 2019. № 2 (22). С. 81-87.

33. Варналій З.С. Економічна безпека та конкурентоспроможність регіонів України : монографія / З.С. Варналій, Р.Р. Білик. Чернівці: Технодрук, 2018. 454 с.

34. Варналій З.С. Механізм попередження загроз економічній безпеці України / З.С. Варналій С.В. Онищенко, О.А. Маслій // Економічний часопис XXI. 2016. № 159 (5 6). С. 20-24. (Scopus, EBSCOhost, Index Copernicus, Ulrich's Periodicals Directory, C.E.E.O.L., RISC). DOI: <http://dx.doi.org/10.21003/ea.V159-04>

35. Веретенникова Г.Б. Економічна безпека підприємства: планування й організація: конспект лекцій / Веретенникова Г.Б. – Х.: Вид. ХНЕУ, 2008. – 84 с.

36. Данільян О.Г. Національна безпека України: структура та напрямки реалізації: навч. посібн./ Данільян О.Г., Дзьобань О.П., Панов М.І. – Х.: Фоліо, 2002. – 285 с.

37. Економічна безпека підприємства в умовах антикризового управління: концептуальне визначення та механізм забезпечення: монографія / А.М. Штангрет, Я.В. Котляревський, М.М. Караїм. Львів: Укр. акад. друкарства, 2012. 288 с.

38. Європа на шляху до інформаційного суспільства: Збірник документів Європейської Комісії 1994-1995 рр. – К.: Державний комітет зв'язку та інформатизації України, 2000. – 120 с.

39. Живко З.Б., Сердюков В.В., Стаднік О.М., Хорошко В.О. Правові основи охорони інформації. Підручник; за ред.проф.В.О.Хорошка. Вид.2. К.: Вид. ДУІКТ, 2009. 355 с.

40. Зегжда Д.П. Как построить защищенную информационную систему / Д.П. Зегжда; под науч. ред. Зегжды Д.П., Платонова В.В. – СПб.: Свет и родина – 95, 1997. – 312 с.

41. Иванов В.Ф. Інформаційне законодавство: український та зарубіжний досвід / В.Ф. Иванов. – К.: Київський ун-т ім. Т.Г. Шевченка. Інститут журналістики, 1999. – 208 с.

42. Кириленко В.І. Інвестиційна складова економічної безпеки: монографія / В.І. Кириленко. – К.: ХНЕУ, 2005. – 232 с.

43. Ковальчук Т.Т. Економічна безпека і політика: із досвіду професійного аналітика / Ковальчук Т.Т. – К.: Знання, 2004. – 638 с.

44. Крысин А.В. Безопасность предпринимательской деятельности/ Крысин А.В. – М.: Финансы и кредит, 1996. – 379 с.

45. Менеджмент безпеки персоналу: конспект лекцій [З.Б.Живко, Л.М.Томаневич, В.С.Дудюк, М.І.Копитко, С.М.Лихолат]; за заг. ред. З.Б.Живко. Львів: Ліга-Прес, 2012. 204 с.

46. Менеджмент безпеки персоналу: навч. посібн. [З. Б. Живко, О. Б. Баворовська, М. О.

- Живко, Л. М. Плахотнюк, Х. З. Босак]; за заг. ред. З. Б. Живко. Львів: Ліга-Прес, 2011. 228 с.
47. Механизмы управления экономической безопасностью/ Лысенко Ю.Г., Мищенко С.Г., Руденский Р.А. и др. – Донецк: ДонНУ, 2002. – 178 с.
48. Мунтіян В.І. Економічна безпека України / В.І. Мунтіян. – К.: Вид. КВІЦ, 1999. – 464 с.
49. Обліково-аналітичне забезпечення управління економічною безпекою підприємства: монографія / За заг. ред. А.М. Штангрета. Львів: Укр. акад. друкарства, 2017. 276 с.
50. Організація перевірок фінансово-господарської діяльності підприємств: підручник [З.Б.Живко, І.О.Ревак, М.О.Живко, С.І.Мельник, Л.М.Плахотнюк]; за заг.ред.З.Б.Живко. – Львів: ЛьвДУВС, 2011. 548 с.
51. Організація та управління системою економічної безпеки підприємства: навчально-методичний посібник [З. Б. Живко, О.В. Черевко, Н.В. Зачосова, М. О. Живко, О.Б. Баворовська, В.О. Занора]; за ред. З.Б. Живко. Черкаси : видавець Чабаненко Ю.А., 2019. 120 с.
52. Основы экономической безопасности: учебн. пособ./ под ред. Олейникова Е.А. – М.: ЗАО «Бизнес-школа» «Интел-Синтез», 1997. – 211 с.
53. Петренко И.Н. Безопасность экономического пространства хозяйствующего субъекта / Петренко И.Н. – М.: Анкил, 2005. – 280 с.
54. Про захист інформації в автоматизованих системах: Закон України// Відомості Верховної ради України. – 1994. – № 31.
55. Протидія злочинам, що вчиняються у бюджетній сфері: навч. посіб. [А.В.Бабяк, З.Б.Живко, А.О.Йосипів, С.І.Марко, Ю.С.Назар]. Львів: ЛьвДУВС, 2010. 168 с.
56. Расторгуев С.П. Философия информационной войны / Расторгуев С.П. – М.: Вуз. книга, 2001. – 468 с.
57. Реверчук Н.Й. Управление экономической безопасностью предприятий структур: монография/ Реверчук Н.Й. – Львів: ЛБІ НБУ, 2004. – 195 с.
58. Соснин А.С. Менеджмент безопасности предпринимательства: учебн. пособ./ Соснин А.С., Пригунов П.Я. – К.: Изд. Европейского университета, 2005. – 240 с.
59. Уткин Э.А. Риск-менеджмент / Уткин Э. А. – М.: ТАНДЕМ, 1998. – 288 с.
60. Фінансова безпека підприємства: навч. посібник / З.С. Варналій, З.Б. Живко, Р.Р. Білик, С.В. Онищенко, М.О. Живко; за ред. З.С. Варналія. Львів: Ліга-Прес, 2018. 300 с.
61. Филин С.А. Информационная безопасность: учебн. пособ. – М.: Изд. «Альфа-Пресс», 2006. – 412 с.
62. Экономическая безопасность: производство – финансы – банки/ Под ред. В.К. Сенчагова. – М.: Финстатинформ, 1998. – 621 с.
63. Ярочкин В.И. Система безопасности фирмы / Ярочкин В.И. – М.: Ось, 2003. – 352 с.
64. Rainbow Series. Dod Trusted Computer Systems Evaluation Criteria / Dod 5200.28 STD – Orange Book.

15. Інформаційні ресурси, у т.ч. в мережі Інтернет

65. Компания Безопасность [Электронный ресурс]. – Режим доступа: <http://bezopasnost.biz>.
66. Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. – Режим доступу: <http://dstszi.gov.ua>.
67. International Charity Foundation for History and Development of Computer Science and Technique, ICFCST. Історія розвитку інформаційних технологій в Україні [Електронний ресурс]. – Режим доступу: http://www.icfcst.kiev.ua/MUSEUM/IT_u.html.
68. Information Technology Security Evaluation Criteria, v. 1.2. – Office for Official publications of the European Communities, 1991 [Електронний ресурс]. – Режим доступу: www.ssi.gouv.fr/IMG/pdf/JILv2.pdf
69. Site of FBI. – Режим доступу: www.fbi.gov.
70. The International PGP Home Page [Electronic resource]. – Access mode: www.pgpi.org.
71. Site of SecurityFocus. – Access mode: www.securityfocus.com.
72. Сайт Sysinternals. – Режим доступу: www.sysinternals.com.
73. [Электронный ресурс]. – Режим доступа: www.zdnet.ru.

74. Журнал «Информационные технологии. Аналитические материалы» [Электронный ресурс]. – Режим доступа: <http://it.ridne.net>.
75. Історія розвитку інформаційних технологій в Україні: нормативні акти України [Електронний ресурс]. – Режим доступу: www.nau.kiev.ua.
76. Розвідка України [Електронний ресурс]. – Режим доступу: <http://rozvidka.livejournal.com/>.
77. Служба безпеки України [Електронний ресурс]. – Режим доступу: <http://www.sbu.gov.ua/>.
78. Служба економічної безпеки [Електронний ресурс]. – Режим доступу: <http://sebweb.at.ua/>.
79. Центр информационных технологий [Электронный ресурс]. – Режим доступа: <http://www.citmgu.ru>.