Ф – М-8.3.01-1

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ВІННИЦЬКИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ ІНСТИТУТ

СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Сертифікована на відповідність ДСТУ ISO 9001:2015 (ISO 9001:2015, IDT)

Кафедра економічної кібернетики та інформаційних систем

ЗАТВЕРДЖЕНО
Постанова вченої ради
26.04.2021
протокол № 4, п. 5

ВВЕДЕНО В ДІЮ
Наказ від 26.04.2021 №82

КІБЕРБЕЗПЕКА / CYBERSECURITY

РОБОЧА ПРОГРАМА

Ступінь вищої освіти	«молодший бакалавр» /	junior bachelor
Галузь знань	12 «Інформаційні технології»/	Information technologies
Спеціальність	126 «Інформаційні системи та технології»/	Information systems and technologies
Освітня програма	«Інформаційні технології у бізнесі» /	Information technologies in business

Вінниця 2021

Розробники: Половенко Людмила, кандидат педагогічних наук, доцент
Яремко Світлана, кандидат технічних наук, доцент

Гарант освітньої програми «Інформаційні технології у бізнесі» – Яремко Світлана, кандидат технічних наук, доцент, доцент кафедри економічної кібернетики та інформаційних систем

Обговорено та схвалено на засіданні кафедри економічної кібернетики та інформаційних систем від 26.03.2021 р. пр. № 04; на засіданні вченої ради факультету економіки, менеджменту та права від 16.04.2021 р. пр. № 5.

Рецензенти: Мерінова Світлана, кандидат економічних, доцент (внутрішня рецензія).

Вапняр Олена - директор ТОВ «Універсальний сервіс» (зовнішнярецензія).

Редактор: Фатєєва Т. Комп'ютерна верстка: Шуляк Н.
Підп. до друку 05.05.2021 р. Формат 60х84/16. Папір офсетний
Друк ксероксний. Ум. друк. арк. 1,91.
Обл.-вид. арк. 1,32. Тираж 5. Зам. № 149.

Редакційно-видавничий відділ ВТЕІ КНТЕУ
21000, м. Вінниця, вул. Хмельницьке шосе, 25

І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Мета вивчення дисципліни

Дисципліна «Кібербезпека» належить до обов'язкових компонентів освітньої програми «Інформаційні технології у бізнесі».

Місце дисципліни у навчальному процесі. Дисципліна «Кібербезпека» викладається на другому курсі у четвертому семестрі загальним обсягом 180 годин / 6 кредитів.

Метою вивчення дисципліни є формування у майбутніх молодших бакалаврів з інформаційних систем та технологій необхідного рівня інформаційної та комп'ютерної культури, здобуття студентами теоретичних знань і набуття практичних навичок з питань організації та забезпечення кібербезпеки; опанування комплексом організаційно-правових, технічних, інформаційних та програмних засобів, що призначені для вирішення широкого кола завдань забезпечення безпеки інформаційних процесів в кфберпросторі.

Вивчення дисципліни включає лекційні, лабораторні заняття та самостійну роботу, що сприяє закріпленню необхідних теоретичних знань та допомагає набуттю практичних навичок для подальшого засвоєння програмних продуктів у роботі за фахом.

Результат вивчення навчальної дисципліни та її місце в освітньому процесі

Результатом вивчення навчальної дисципліни «Кібербезпека» для освітньої програми «Інформаційні технології у бізнесі» є формування комплексу компетентностей:

- **інтегральна компетентність:**

здатність розв'язувати складні спеціалізовані завдання та практичні проблеми у сфері публічного управління та адміністрування або у процесі навчання, що передбачає застосування теорій та наукових методів відповідної галузі і характеризується комплексністю та невизначеністю умов;

- **загальні компетентності:**

КЗ 1. Здатність до логічного мислення.

КЗ 2. Здатність накопичувати, обробляти, систематизувати та застосовувати знання у практичних ситуаціях.

КЗ 3. Розуміння предметної області та професійної діяльності.

КЗ 5. Здатність до навчання та здобуття сучасних знань.

КЗ 6. Здатність здійснювати пошук, оброблення та узагальнення інформації з різних джерел.

КЗ 8. Здатність проводити дослідження та формулювати висновки.

КЗ 10. Здатність до усвідомлення моральних, культурних, наукових цінностей на основі розуміння історії та закономірностей розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для відпочинку та ведення здорового способу життя.

- **спеціальні (фахові, предметні) компетентності:**

КС 1. Здатність застосовувати фундаментальні та міждисциплінарні знання для успішного розв'язання завдань у галузі інформаційних систем та технологій.

КС 3. Здатність до використання та налагодження системного, комунікаційного та апаратно-програмного забезпечення інформаційних систем.
КС 6. . Здатність використовувати методи і засоби забезпечення інформаційної та функціональної безпеки в області інформаційних систем та технологій.
КС 9. Здатність застосовувати сучасні інформаційно-комунікаційні системи та технології (у тому числі такі, що базуються на використанні Інтернет).
КС 12. Здатність узагальнювати та презентувати результати досліджень у сфері інформаційних систем та технологій.

Програмні результати навчання здобувачів з навчальної дисципліни «Кібербезпека»:

ПР 2. Вміти знаходити аналогії та застосовувати знання, вміння та навички з суміжних дисциплін для формування та розв'язання професійних задач в області інформаційних систем та технологій.
ПР 4. Користуватися сучасними інформаційно-комунікаційними системами та технологіями, у тому числі такими, що базуються на використанні Інтернет.
ПР 6. Знати основи забезпечення інформаційної та функціональної безпеки, види кіберзагроз і застосовувати їх на практиці під час впровадження та супроводу інформаційних систем.
ПР 9. Аналізувати та узагальнювати необхідну інформацію з різних джерел та ресурсів для вирішення професійних задач з урахуванням сучасних досягнень науки і техніки.

Міждисциплінарні зв'язки: програма упорядкована відповідно до анотації освітньо-професійної програми підготовки бакалаврів, базується на вивченні дисциплін «Офісні комп'ютерні технології», «Комп'ютерні мережі» і передує вивченню нормативних дисциплін «Технології бізнес-аналітики», «Інтернет речей».
Знання, отримані здобувачами вищої освіти під час вивчення дисципліни «Кібербезпека» є базою для опанування дисциплін циклу професійної підготовки, а також можуть бути застосовані під час проходження виробничої практики, підготовки курсових та кваліфікаційних робіт за спеціальністю.
Отже, у результаті вивчення цієї дисципліни здобувач вищої освіти зможе використовувати набуті навички застосування сучасних методів і засобів кібербезпеки, що дає можливість для вирішення низки актуальних завдань, що передбачають розроблення, впровадження та експлуатацію захищених інформаційних і комунікаційних систем.

Критерії оцінювання результатів навчання

Рівні компетентності	**За шкалою КНТЕУ**	**Критерії оцінювання**
1	2	3
Високий (дослідницький)	90-100	Має обґрунтовані та всебічні знання з дисципліни, вміє узагальнювати та систематизувати набуті знання; самостійно знаходить джерела інформації та працює з ними; проводить власні дослідження, може використовувати набуті знання та вміння при розв'язанні задач.
Достатній (частково-пошуковий)	82-89	Володіє навчальним матеріалом, вміє зіставляти та узагальнювати, виявляє творчий інтерес до предмету, виконує завдання з повним поясненням та обґрунтуванням, але допускає незначні помилки; може усвідомити нові для нього факти, ідеї.
	75-81	Володіє визначеним програмою навчальним матеріалом; розв'язує завдання, передбачені програмою, з частковим поясненням.
Елементарний (репродуктивний)	69-74	Володіє навчальним матеріалом на репродуктивному рівні; може самостійно розв'язати та пояснити розв'язання завдання.
	60-68	Ознайомлений з навчальним матеріалом, відтворює його на репродуктивному рівні; виконує елементарні завдання за зразком або відомим алгоритмом.
Низький (фрагментарний)	35-59	Ознайомлений та відтворює навчальний матеріал на рівні окремих фактів та фрагментів матеріалу; під керівництвом викладача виконує елементарні завдання.
	1-34	Ознайомлений з навчальним матеріалом на рівні розпізнавання та відтворення окремих фактів.

Якщо здобувач вищої освіти повністю виконав програму дисципліни та набрав протягом семестру 75 і більше балів, то підсумкова оцінка може бути виставлена без опитування чи виконання екзаменаційного завдання на момент проведення екзамену.

У разі, якщо здобувач вищої освіти бажає поліпшити свою оцінку, або не набрав 75 балів, він складає екзамен з усієї програми навчальної дисципліни у вигляді письмового опитування знань згідно завдань встановленого зразка.

Результат виконання екзаменаційних завдань оцінюється з урахуванням результатів у співвідношенні 80:20, де 80 – максимальна оцінка за виконання екзаменаційного завдання, 20 – результат поточної успішності відповідно до шкали переводу поточної роботи для врахування її при підсумковій оцінці.

Обсяг дисципліни в кредитах та його розподіл (тематичний план)

Назва теми	Кількість годин				Форми контролю
	Всього год./ кредит.	з них			
		Лекції	Лабораторні	Самостійна робота	
Тема 1. Основні положення теорії кібербезпеки	13	2	2	9	УО, СУН, КТ
Тема 2. Поняття та зміст кіберзагроз	13	2	2	9	УО, СУН, КТ
Тема 3. Методи зламу комп'ютерних мереж	13	2	4	7	ЕЗ, ІЗ, ПО
Тема 4. Організаційно-правове забезпечення захисту інформації	13	2	4	7	Р, СУН
Тема 5. Побудова систем захисту від загроз порушення конфіденційності інформації	13	2	4	7	ЕЗ, ІЗ, ОЗ
Тема 6. Побудова систем захисту від загроз порушення цілісності	13	2	4	7	ІЗ, ОЗ, ПО
Тема 7. Побудова систем захисту від загроз порушення доступності	13	2	4	7	ЕЗ, ІЗ, ОЗ
Тема 8. Аналіз основних загроз інформаційних потоків підприємства	13	2	4	7	ІЗ, ОЗ,СУН
Тема 9. Організація інформаційної безпеки на підприємстві	11	2	2	7	ЕЗ, ІЗ, ОЗ, ПО
Тема10. Криптографічні методи захисту інформації	13	4	2	7	ЕЗ, ІЗ, ОЗ
Тема 11. Методи криптоаналізу	15	4	4	7	ЕЗ, ІЗ, ПО
Тема 12. Захист від шкідливого програмного забезпечення	13	4	4	5	ЕЗ, Т, СУН
Тема 13. Захист мережевого керування	12	4	4	4	ЕЗ, ІЗ, ОЗ
Тема 14. Перспективні напрями розвитку комплексів засобів захисту інформації	12	4	4	4	Р, ПО, Т
Разом	**180/6**	**38**	**48**	**94**	
Підсумковий контроль	**екзамен**				

Умовні позначення: УО/ПО - усне/письмове опитування; ЕЗ - вирішення задач в електронному вигляді; ІЗ - індивідуальне завдання; Т – тестування; Р- підготовка реферату; ОЗ - оформлення звітів та захист робіт, ПКР – підсумкова контрольна робота, СУН- використання системи управління навчанням Moodle, КТ – комп'ютерне тестування.

ІІ. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст дисципліни (теми програми)

Тема 1. Основні положення теорії кібербезпеки

Концептуальні засади забезпечення інформаційної безпеки України. Основні визначення і поняття теорії захисту інформації. Основні поняття захисту інформації: речова, телекомунікаційна та документована інформація. Інформаційні ресурси й процеси.

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

Методи і способи захисту інформації. Основні напрями забезпечення безпеки: правовий, організаційний та технічний захист. Керування захистом інформаційних об'єктів.

Тема 2. Поняття та зміст кіберзагроз

Аналіз погроз інформаційній безпеці, проблеми інформаційної війни. Інформаційні механізми впливу в сучасній політиці. Основні етапи виникнення та розвитку конфліктів в сучасному інформаційному суспільстві.

Реальність, дійсність та дієвість інформаційно-психологічних операцій сьогодення. Мас-медійні гравці та тероризм в системі засобів масової інформації. Інструментарій іміджології у веденні інформаційних воєн.

Форми і засоби ведення інформаційної боротьби в кіберпросторі. Класифікація та основні характеристики загроз інформаційній безпеці.

Уразливість інформації. Основні групи загроз: порушення цілісності, конфіденційності та доступності інформації. Зловмисники та випадкова втрата даних. Проблема забезпечення кібербезпеки. Загальнометодологічні принципи теорії інформаційної безпеки. Методи й засоби забезпечення інформаційної безпеки. Визначення політики безпеки.

Тема 3. Методи зламу комп’ютерних мереж

Інтернет як новітня мережа загальносвітового поширення інформації. Розвиток інформаційних технологій, мережі Інтернет та обумовлені ними проблеми інформаційної безпеки. Електронний екстремізм, електронний тероризм, кіберзлочинність та кібертероризм. Медіа тероризм та Інтернет.

Інформаційні загрози мережевих комунікацій. Поняття атаки на комп'ютерну систему. Виконання атак та виявлення методів ненаправлених і направлених хакерських атак. Характеристика каналів комунікативного впливу на свідомість суспільства.

Тема 4. Організаційно-правове забезпечення захисту інформації

Загрози національній безпеці держави в інформаційній сфері. Інформаційна політика держави в умовах інформаційної війни. Поняття державно-правового механізму інформаційної безпеки. Принципи правового регулювання напрямків інформаційної безпеки. Правове регулювання суспільних відносин в інформаційній сфері. Напрями державної інформаційної політики. Особливості застосування методів державного управління в сферіінформаційної безпеки.

Використання інформаційних технологій у процесі державного управління: «електронний уряд», зміна ролі та статусу ЗМІ у процесі державного управління. Система органів державної влади як основний керуючий фактор у вирішення конфліктів в інформаційній сфері. Державна система інформаційного протиборства.

Особливості захисту електронної корпоративної інформації. Міжнародні стандарти безпеки інформаційно-обчислювальних систем. Вітчизняні державні стандарти технічного захисту інформації. Законодавча класифікація видів інформації в Україні. Державна таємниця як особливий вид інформації, що захищається. Конфіденційна інформація. Система захисту державної таємниці. Правовий режим захисту державної таємниці. Ліцензійна й сертифікаційна діяльності в сфері інформаційної безпеки. Нормативна база в галузі захисту програмних продуктів від несанкціонованого використання.

Основні проблеми правого регулювання мережі Інтернет. Режими доступу до інформації. Обмеження доступу до інформації в інтересах слідства та судочинства. Обмеження щодо виробництва та ввезення в Україну інформаційної продукції. Інформаційна безпека громадян як суб'єктів політичного процесу.

Вимоги вітчизняних стандартів захисту конфіденційної інформації від несанкціонованого доступу під час обробки в автоматизованих системах.

Правові основи захисту інформації з використанням застосування технічних засобів (захисту від технічних розвідок, застосування й розробка шифрувальних засобів і т. д.). Захист інтелектуальної власності засобами патентного й авторського права.

Зарубіжна нормативна база в галузі технічного захисту інформації. Відомі міжнародні стандарти управління інформаційною безпекою: 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 Infra-structure Library (ITIL) и Statement on Auditing Standards (SAS) No. 70. Критерії, вимоги та категорії систем безпеки «Оранжевої книги».

Тема 5. Побудова систем захисту від загроз порушення конфіденційності інформації

Перелік конфіденційних відомостей організації. Порядок проведення експертизи з метою визначення конфіденційності інформації. Дослідження структури та умов функціонування ІС організації.

Організаційні заходи та заходи забезпечення фізичної безпеки.

Захист інформації від витоку технічними каналами. Захист інформації в комп'ютерних системах та мережах.

Системи аутентифікації та ідентифікації. Класифікація систем аутентифікації та ідентифікації. Особливості електронних системаутентифікації та ідентифікації.

Використання паролів. Особливості парольних систем аутентифікації. Властивості, достоїнства та недоліки використання парольного захисту.

Розрахунок стійкості парольного захисту інформації. Використання парольного захисту інформації в різних системах.

Розмежування доступу до інформації в залежності від повноважень користувача.

Захист авторських прав в інформаційних системах. Патентне та авторське право в Україні та світовій практиці. Захист елементів інформаційних систем патентами. Комп'ютерні програми і бази даних як об'єкти захисту авторського права.

Тема 6. Побудова систем захисту від загроз порушення цілісності

Принципи забезпечення цілісності. Структура системи захисту від загроз порушення цілісності.

Криптографічні методи забезпечення цілісності інформації. Основи електронного цифрового підпису. Порядок використання цифрового підпису. Правила сертифікації ключів.

Поняття про хеш-функції. Коди перевірки автентичності.

Методи ідентифікації програм та захист авторських прав.

Особливості захисту офісних електронних документів від несанкціонованої модифікації та розповсюдження. Методика та заходи захисту. Оптимізації заходів захисту. Критерії оптимізації. Використання економічного підходу при оптимізації засобів захисту.

Тема 7. Побудова систем захисту від загроз порушення доступності

Захист мовленнєвої інформації, що передається у відкритих каналах зв’язку. Стеганографічні методи захисту письмової інформації, що передається у відкритих каналах зв’язку.

Структура системи захисту від загроз порушення доступності Дублювання шлюзів і міжмережевих екранів. Резервне копіювання інформації. Вибір програм розмежування доступу до інформації.

Відмовостійкість дискової підсистеми. Використання RAID технологій.

Відмовостійкість серверів.

Аналіз існуючих методів і засобів, застосовуваних для контролю й захисту інформації, і розробка пропозицій щодо їхнього вдосконалення й підвищення

Методи та засоби захисту систем управління базами даних. Причини, види, основні методи порушення конфіденційності в системах управління базами даних (СУБД). Одержання несанкціонованого доступу до конфіденційної інформації шляхом логічних висновків. Методи захисту СУБД. Особливості керування доступом: потоковий, контроль висновку, контроль доступу; багаторівневий захист. Підтримка логічної цілісності, транзакції функціонування, синхронізація в розподілених СУБД. Забезпечення безпеки багаторівневих реляційних СУБД. Кластерна організація серверів баз даних. Особливості реалізації механізмів захисту деяких комерційних СУБД.

Тема 8. Аналіз основних загроз інформаційних потоків підприємства

Концепція безпеки підприємства. Система інформаційної безпеки підприємства. Служба безпеки фірми (підприємства, організації, установи). Недобросовісна конкуренція і захист комерційної таємниці. Ділова (корпоративна) розвідка.

Приклади сценаріїв злому інформаціної системи на підприємстві. Наслідки порушення інформаційної безпеки на підприємстві. Основні закони та положення України, які регламентують відповідальність за порушення інформаційної безпеки.

Нормативні документи на підприємстві для організації безпеки інформаційних технологій. Основні заходи щодо організації спеціального діловодства з носіями інформації.

Тема 9. Організація інформаційної безпеки на підприємстві

Поняття політики безпеки (ПБ) на підприємстві. Служби інформаційної безпеки (ІБ) на підприємстві. Типові функціональні обов’язки співробітників служби ІБ. Методика розробки ПБ на підприємстві. Основні етапи реалізації ПБ в умовах сучасного бізнесу.

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.

Порядок проведення робіт з технічного захисту інформації. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

Роботи, які пов’язані із розробкою й аналізом засобів забезпечення інформаційної безпеки комп’ютерних систем на основі розроблених програм і методик, у тому числі із забезпеченням вимог, що випливають із документів, що регламентують режим дотримання державної таємниці.

Організація оптимального використання парольного захисту інформації на підприємстві.

Організація на підприємстві групи влагоджування інцидентів комп’ю- терної безпеки. Її права, статус, обов’язки. Порядок й організація проведення розслідування за фактом комп’ютерного інциденту.

Тема 10. Криптографічні методи захисту інформації

Сутність та історія розвитку криптографії. Класифікація методів шифрування. Стійкість шифрів. Криптографічні хеш-функції.

Загальні схеми блокового і потокового шифрування. Стандарти симетричного шифрування DES.

Сутність і завдання асиметричного шифрування. Алгоритм шифрування асиметричного шифрування RSA.

Електронний цифровий підпис. Робота з програмами шифрування на відкритому ключі. Освоєння програмних засобів електронного цифрового підпису.

Реалізація криптографічних методів захисту інформації. Управління ключами. Шифрування потоків даних і повідомлень великого обсягу. Використання «блукаючих ключів». Шифрування, завадостійке кодування і стиснення інформації.

Вибір програм автоматичного шифрування інформації при її збереженні на дисках та відпрацювання практичних навичок їх застосування.

Використання криптографічного захисту електронної пошти.

Тема 11. Методи криптоаналізу

Основи криптоаналізу. Робота з програмами криптографічного закриття інформації. Основні типи криптоаналітичного розкриття. Методи криптоаналізу. Робота з програмами криптографічного закриття інформації. Освоєння прикладних програм «прозорого» шифрування.

Дослідження програмних засобів криптографічного захисту інформації. Аналіз алгоритмів симетричного шифрування. Алгоритм DES. Алгоритм ГОСТ 28147-89. Алгоритм AES. Аналіз алгоритмів асиметричного шифрування. Алгоритм RSA. Алгоритм Рабіна. Алгоритм Ель Гамаля. Аналіз алгоритмів електронного цифрового підпису. Алгоритм RSA. Алгоритм Ель Гаміль. Алгоритм ГОСТ Р 34.10-2001.

Побудова хеш-функцій. Хеш-функції на основі блокових шифрів. Самостійні хеш-алгоритми.

Тема 12. Захист від шкідливого програмного забезпечення

Особливості забезпечення захисту ком'ютерних систем сполучених з глобальною мережею Інтернет. Типи та класифікація загроз, відповдно популярним сервісам. Вразливості протоколів Інтернет. Особливості загрози типу „відмова в обслуговувані". Характеристика інструментальних засобів захисту. Політика безпеки при використанні ресурсів мережі Інтернет.

Руйнуючі програмні засоби. Програми з потенційно шкідливим впливом та їх властивості. Основні класи руйнуючих програм. Захист інформації у комп'ютерах від вірусів. Методи захисту від шкідливих програм. Тестовий вірус. Програмні засоби захисту інформації. Вибір та застосування антивірусних програм. Політика безпеки при опрацюванні електронної пошти. Захист електронної пошти від спаму. Визначення та класифікація спаму. Особливості

«фішінгу». Модель загроз від спаму. Методи розпізнавання спаму: чорні та білі списки, баєсовський підхід. Використання методів штучного інтелекту для розпізнавання спаму. Методи та засоби протидії спаму.

Тема 13. Захист мережевого керування

Модель мережевого керування, яка використовується у протоколі SNMP. Основні принципи роботи протоколу SNMP. Об'єднання SNMPv1 як засоби захисту. Протокол SNMPv2. Конфігурація модуля посередника (система proxy). Архітектура протоколу SNMPv3. Розподілене мережеве керування. Модель обробки повідомлень і захисту користувача. Обробка повідомлення в моделі USM.

Тема 14. Перспективні напрями розвитку комплексів засобів захисту інформації

Адаптивні комплекси засобів захисту інформації: активні системи захисту, системи виявлення вторгнень; системи керування захищеністю; комплекси засобів захисту інформації мобільних програмних систем.

Передумови створення активних систем захисту інформації. Методика зменшення ефективності атак та збільшення ефективності захисту за рахунок використання обчислювальних ресурсів порушника.

Основи систем аналізу вразливостей. Інформаційні сховища вразливостей та їх застосування. Системи аналізу вразливостей провідних світових виробників. Основи систем виявлення вторгнень. Системи виявлення вторгнень провідних світових виробників. Використання засобів штучного інтелекту для діагностики вразливостей та вторгнень в розподілені системи та мережі.

Механізми та засоби захисту програм та електронного документообігу від несанкціонованої модифікації та розповсюдження.

Безпека мобільного програмного забезпечення та мобільних пристроїв. Характеристика специфічних загроз. Особливості захисту мобільних програмних компонентів та систем мобільних програмних агентів. Задачі

захисту мобільного програмного забезпечення та платформи його функціонування. Особливості системи безпеки COM/DCOM, ActiveX, Java, Framework, Flash Macromedia.

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

Структура навчальної дисципліни

Результати навчання	*Навчальна діяльність*	*Робочий час студента год.*
1	**2**	**3**
Знати та розуміти: основні положення теорії кібербезпеки. Оволодіти понятійним апаратом: інформація, конфіденційність, цілісність, доступність, захист інформації, інформаційна безпека. Опанувати основні напрями забезпечення безпеки: правовий, організаційний та технічний захист. **Вміти:** здійснювати профілактичну та попереджувальну діяльність по відношенню до інформаційних загроз на рівні особистої інформаційної безпеки.	**Тема 1: Основні положення теорії кібербезпеки**	13
	Лекція 1 План лекції: 1. Поняття та зміст інформаційної безпеки. 2. Сфери застосування та методи захисту інформації. 3. Основні характеристики інформації: конфіденційність, цілісність та доступність. 4. Методи і способи захисту інформації. **Література:** Основна: 2, 3, 5, 7, 8. Додаткова: 15, 18, 24, 27, 28, 32. Інтернет-ресурси: 34, 35.	2
	Самостійна робота: Глобалізація як визначальний процес розвитку сучасного світу. Загрози та виклики інформаційної епохи. Інформаційні механізми впливу в сучасній політиці. Інформаційні війни. Основні напрямки захисту інформаційної безпеки людини та суспільства.	7
	Лабораторна робота 1: Створення досьє План: 1. Створити досьє з використанням інтернет- ресурсів для оцінки впливу ІКТ-технологій на недоторканість приватного життя. 2. Знайти як можна більше особистої інформації про колегу, використовуючи загальнодоступні мережеві ресурси. 3. Оцінити можливість використання знайденої інформації зловмисниками. 4. Надати рекомендації по забезпеченню необхідного рівня безпеки приватного життя у світі цифрових залежностей.	2
	Лабораторна робота 2: Налаштування двофакторної авторизації План: 1. Налаштувати двохфакторну авторизацію для захисту власної електронної пошти. 2. Налаштувати двохфакторну авторизацію для захисту акаунтів соціальних мереж.	2

1	2	3
Знати та розуміти: Основні класи кіберзагроз. Проблеми, обумовлені розвитком інформаційних технологійта мережі Інтернет. Оволодіти понятійним апаратом: комп'ютерний тероризм, кібертероризм, інформаційний тероризм, мережеві війни. **Вміти:** перевіряти, чи сертифікати систем комп'ютерної безпеки задовольняють потребам індустрії безпеки; оцінювати існуючі операційні системи відповідно до критеріїв "Помаранчевої книги"; виявляти можливі шляхи атаки інформації або комп'ютерної системи.	**Тема 2: Поняття та зміст кіберзагроз**	13
	Лекція 2 План лекції: 1. Інформаційні механізми впливу в сучасній політиці. Інформаційні війни. 2. Основні класифікації загроз інформаційній безпеці. 3. Загрози безпеки: за засобами впливу на систему, в розподільчих системах. 4. Інформаційні загрозимережевих комунікацій. **Література:** Основна: 2, 4, 8. Додаткова: 11, 14, 15, 18, 19, 29, 32. Інтернет-ресурси: 34, 36.	2
	Самостійна робота: Основні етапи виникнення та розвитку конфліктів в сучасному інформаційномусуспільстві. Реальність, дійсність та дієвість інформаційно-психологічних операцій сьогодення. Мас-медійні гравці та тероризм в системі засобів масової інформації. Інструментарій іміджології у веденні інформаційних воєн.	7
	Лабораторна робота 3: Перевірка сертифікатів комп'ютерної безпеки План: 1. Визначити функціональний рівень системи. 2. Перевірити вимоги гарантованості і документування.	2
	Лабораторна робота 4: Перевірка сертифікатів комп'ютерної безпеки План: 1. Перевірити вимоги гарантованості і документування. 2. Запропонувати способи виявлення атак.	2

1	2	3
Знати та розуміти: методи зламу, види атак, ненаправлені та направлені хакерські атаки. **Вміти:** визначати IP-адреси веб-сервера, поштового сервера та іншої інформації. Виявляти можливі шляхи атаки інформації або комп'ютерної системи.	**Тема 3: Методи зламу комп'ютернихмереж**	13
	Лекція 3 План лекції: 1. Історія методів зламу. 2. Вивчення сучасних методів. 3. Виконання атак. 4. Виявлення методів направлених на ненаправлених атак. **Література:** Основна: 2, 8. Додаткова: 13, 14, 22, 24. Інтернет-ресурси: 34.	2
	Самостійна робота: Як зловмисник може використовувати фізичні засоби для отримання інформації або для її знищення. Використання економічного підходу при оптимізації засобів захисту.	7
	Лабораторна робота 5: Виявлення атакПлан: 1. Визначити IP-адресу веб-сервераінституту. 2. Визначите IP-адресу поштовогосервера. 3. Відправити ping-пакети та просканувати адресний простір.	2
	Лабораторна робота 6: Виявлення атак План: 1. Визначити IP-адресу веб-сервераінституту. 2. Визначите IP-адресу поштовогосервера. 3. Дізнатися, які хости зараз знаходяться в режимі онлайн.	2

1	2	3
Знати: основи нормативно-правого регулювання питань національної безпеки в Україні. Нормативно-правові акти, що визначають функції держави із захисту інформаційної безпеки. визначати фактори, що впливають на формування політики інформаційної безпеки; розробляти заходи економічної безпеки. **Вміти:** здійснювати огляд можливостей захисту на рівні комунікаційних протоколів; оцінювати їх архітектуру, принципи адресації, маршрутизації	**Тема 4: Організаційно-правове забезпечення захисту інформації**	13
	Лекція 4 План лекції: 1. Поняття державно-правового механізму інформаційної безпеки. 2. Напрями державної інформаційної політики. 3. Нормативні документи системи технічного захисту інформації. 4. Законодавча класифікація видів інформації в Україні. **Література:** Основна: 4. Додаткова: 11, 18, 20, 21, 26. Інтернет-ресурси: 35.	2
	Самостійна робота: Система інформаційної безпеки та принципи її побудови. Захист персональних даних. Інформаційна безпека України у сфері прав і свобод людини. Недобросовісна конкуренція і захист комерційної таємниці.	7
	Лабораторна робота 7: Захист на рівні комунікаційних протоколів План 1. Переглянути облікові записи користувачів за допомогою утиліти net. 2. Переглянути всі відкриті ресурси за допомогою команди net share. 3. Переглянути всі динамічні записи системної ARP-таблиці.	2
	Лабораторна робота 8: Захист на рівні комунікаційних протоколів План 1. Дослідити, які атаки можна реалізувати, використовуючи недоліки ARP-Протоколу. 2. Яким чином можна захиститися від атак на рівні комунікаційних протоколів? 3. Чому виникла необхідність у введені протоколу IPv6? 4. Для чого використовується служба DNS? Які атаки можна реалізувати на цю службу?	2

1	2	3
	Тема 5: Побудова систем захисту від загроз порушення конфіденційності інформації	13
Знати: порядок проведення експертизи з метою визначення конфіденційності інформації; основи та методику побудови систем захисту інформації від загроз порушення конфіденційності; принципи розробки програмних засобів зламу парольного захисту. **Вміти:** оцінювати стійкість парольного захисту, здійснювати розмежування доступу до інформації; навчитись захищатися від флуд-атак.	**Лекція 5** План лекції: 1. Причини, види, основні методи порушення конфіденційності. 2. Системи аутентифікації та ідентифікації. Розрахунок стійкості парольного захисту інформації. 3. Розмежування доступу до інформації в залежності від повноважень користувача. 4. Призначення й основні можливості протоколу IPSec. **Література:** Основна: 3, 4, 7, 8. Додаткова: 11, 14, 20-26, 29. Інтернет-ресурси: 34-36.	2
	Самостійна робота: Захист авторських прав в інформаційних системах. Патентне та авторське право в Україні та світовій практиці. Захист елементів інформаційних систем патентами.	7
	Лабораторна робота 9: Захист IP План: 1. Дослідження стійкості парольного захисту. 2. Багатофакторна авторизація.	2
	Лабораторна робота 10: Захист IP План: 1. Реалізація та захист від флуд-атак. 2. Особливості керування доступом: потоковий, контроль висновку, контроль доступу; багаторівневий захист.	2

1	2	3
Знати та розуміти: основи та методику побудови систем захисту інформації від загроз порушення цілісності. Оволодіти понятійним апаратом: коректність транзакцій, мінімізація привілеїв, аудит подій, електронний цифровий підпис, криптографічні хеш-функції, коди перевірки автентичності; технології атак рівня *WEB*. **Вміти:** налаштовувати систему керування доступом ОС Windows; використовувати систему реєстрації подій; змінювати параметри безпеки користувачів та групи коирстувачів; здійснювати захист від атак рівня *WEB* на основі принципів їх реалізації; здійснювати інсталяцію та налаштування Веб-серверу, серверних додатків; визначати стійкість Веб-серверу при атаці на звичайну HTML сторінку та серверний додаток.	**Тема 6: Побудова систем захисту від загроз порушення цілісності**	13
	Лекція 6 План лекції: 1. Принципи забезпечення цілісності. 2. Правила сертифікації ключів. 3. Поняття про хеш-функції. Коди перевірки автентичності. 4. Методи ідентифікації програм та захист авторських прав. **Література:** Основна: 5, 6, 10. Додаткова: 11-14, 22, 24, 25,31. Інтернет-ресурси: 34.	2
	Самостійна робота: Методи та засоби захисту СУБД. Причини, види, основні методи порушення конфіденційності в СУБД. Одержання несанкціонованого доступу до конфіденційної інформації шляхом логічних висновків. Особливості керування доступом: потоковий, контроль висновку, контроль доступу; багаторівневий захист. Підтримка логічної цілісності,транзакції функціонування, синхронізація в розподілених СУБД. Забезпечення безпеки багаторівневих реляційних СУБД. Кластерна організація серверів баз даних. Особливості реалізації механізмів захисту деяких комерційних СУБД.	7
	Лабораторна робота 11: Керування параметрами безпеки сучасних ОС. План: 1. Проблеми безпеки WEB. 2. Загрози безпеки WEB. 3. Методи захисту WEB.	2
	Лабораторна робота 12: Керування параметрами безпеки сучасних ОС. План: 1. Загрози безпеки WEB. 2. Методи захисту WEB.	2

1	2	3
Знати та розуміти: основи та методику побудови систем захисту інформації від загроз порушення доступності на етапах отримання, обробки, збереження та передачі інформації. **Вміти:** отримувати сертифікати та забезпечувати захист засобами SSL веб-сайта на сервері IIS (Internet Information Server).	**Тема 7: Побудова систем захисту від загроз порушення доступності**	13
	Лекція 7 План лекції: 1. Структура системи захисту від загроз порушення доступності. 2. Дублювання шлюзів і міжмережевих екранів. 3. Резервне копіювання інформації. 4. Використання RAID технологій та дзеркалювання серверів. **Література:** Основна: 5, 6, 10. Додаткова: 11-14, 22, 24, 25,31. Інтернет-ресурси: 34.	2
	Самостійна робота: Особливості захисту офісних електронних документів від несанкціонованої модифікації та розповсюдження. Методика та заходи захисту. Оптимізації заходів захисту. Критерії оптимізації. Використання економічного підходу при оптимізації засобів захисту.	7
	Лабораторна робота 13: Захист на рівні протоколів TLS/SSL План: 1. Установити Certificate Services. 2. Створити сертифікат, додати центр сертифікації (Certificate Authority) в список довірених. 3. За допомогою сертифіката захистити створений віртуальний каталог.	2
	Лабораторна робота 14: Захист на рівні протоколів TLS/SSL План: 1. Створити сертифікат, додати центр сертифікації (Certificate Authority) в список довірених. 2. За допомогою сертифіката захистити створений віртуальний каталог.	2

1	2	3
Знати: основи організації захисту інформації на підприємстві; принципи організації роботи з персоналом, який володіє інформацією з обмеженим доступом; особливості організації спеціального діловодства на підприємстві. **Вміти:** планувати й організовувати роботу по створенню і розвитку комплексної системи інформаційної безпеки комерційних підприємств, банків; виконувати роботу по забезпеченню інформаційної безпекиу роботі з персоналом підприємства.	**Тема 8: Аналіз основних загроз інформаційних потоків підприємства**	13
	Лекція 8 План лекції: 1. Основи організації захисту інформації на підприємстві. 2. Принципи організації роботи з персоналом, який володіє інформацією з обмеженим доступом. 3. Особливості організації спеціального діловодства на підприємстві. 4. Ділова (корпоративна) розвідка. **Література:** Основна: 5, 6, 9, 10. Додаткова: 12.	2
	Самостійна робота: Спеціальне діловодство на підприємстві. Особливості захисту офісних електронних документів від несанкціонованої модифікації та розповсюдження.	7
	Лабораторна робота 15: Політика інформаційної безпеки віртуального підприємства План: 1. Вивчити шаблони документів, які описують політику ІБ організації. 2. Вивчити статут, основні положення та стратегічні цілі підприємства (відповідних підрозділів). 3. Підібрати найбільш вдалий шаблон для опису політики безпеки, при необхідності модифікувати його структуру.	2
	Лабораторна робота 16: Політика кібербезпеки віртуального підприємства План: 1. При необхідності модифікувати структуру. шаблону для опису політики кібербезпеки. 2. Розробити політику кібербезпеки з урахуванням специфіки діяльності та планів розвитку підприємства (підрозділу).	2

1	2	3
Знати: методику розробки політики безпеки підприємства; типову структуру підсистем безпеки. **Вміти:** визначати статус інформації (комерційна таємниця, службова інформація, фінансова інформація, для внутрішнього використання, загальнодоступна тощо); оптимізувати систему захисту інформації; встановлювати права доступу різним групам користувачів і оперативно вносити зміни в політику безпеки інформаційної системи.	**Тема 9: Організація інформаційної безпеки на підприємстві**	13
	Лекція 9 План лекції: 1. Організація політики безпеки (ПБ) на підприємстві. 2. Міжнародні стандарти управління ІБ. 3. Організація оптимального використання парольного захисту інформації на підприємстві. 4. Організація ефективної системи безпеки підприємства. **Література:** Основна: 5, 6, 9, 10. Додаткова: 12.	2
	Самостійна робота: Обмеження доступу до інформації в інтересах слідства та судочинства. Особливості захисту інформації під час розслідування кримінальних справ.	7
	Лабораторна робота 17: Побудова політики безпеки підприємства План: 1. Проаналізувати структуру підприємства (загальну кількість працівників, відділів та їх взаємодію). 2. Розробити структурну схему підприємства, вказавши всі відділи та працівників, їх посади та функціональні обов'язки, пов'язані з використанням ІТ та комп'ютерних мереж. 3. Проаналізувати інформаційні потоки, які існують всередині підприємства (зовнішні та внутрішні, а також інформаційні потоки, які використовуються для обміну даними між різними відділами).	2
	Лабораторна робота 18: Безпека підприємства План: 1. Виділити потоки з інформацією, що потребує захисту, визначити її статус (комерційна таємниця, службова інформація, фінансова інформація, лише для внутрішнього використання, загальнодоступна тощо). 2. Побудувати таблицю розмежування доступу для різних категорій працівників або відділів. 3. Розробити політику кібербезпеки верхнього рівня підприємства.	2

1	2	3
Знати та розуміти: сутність та історія розвитку криптографії; методику та процедуру шифрування з використанням різних видів шифрів; сутністьі завдання асиметричного шифрування; основні поняття та створення ключів в алгоритмі асиметричного шифрування RSA. **Вміти:** здійснювати шифрування та дешифрування інформації з використанням різних видів шифрів.	**Тема 10: Криптографічні методи захисту інформації**	13
	Лекція 10 План лекції: 1. Криптографічні методи захисту інформації. 2. Розвиток технологічних засобів криптографії. 3. Загальна класифікація класичних шифрів. **Лекція 11** План лекції: 1. Симетричні шифри. 2. Асиметричні шифри. 3. Потокове та блочне шифрування. 4. Технологія цифрового підпису. **Література:** Основна: 1. Додаткова: 30. Інтернет-ресурси: 33, 37-39.	2 2
	Самостійна робота: Реалізація криптографічних методів захисту інформації. Управління ключами. Шифрування потоків даних і повідомлень великого обсягу. Використанн «блукаючих ключів». Шифрування, завадостійке кодування і стиснення інформації.	7
	Лабораторна робота 19: Криптографічні методи захисту інформації План: 1. Зашифрувати повідомлення за допомогою послідовності літер. 2. Зашифрувати повідомлення за допомогою шифру Цезаря. 3. Зашифрувати повідомлення, скориставшись шифром Віженера. 4. Подати слово у цифровій формі, замінивши кожен символ тексту його номером у алфавіті.	2
	Лабораторна робота 20: Криптографічні методи захисту інформації План: 1. Для відкритого тексту провести закодування табличним методом. 2. Для відкритого тексту провести закодування методом частоколу.	2

1	2	3
Знати та розуміти: оволодіти понятійним апаратом: крипто аналіз, розсіювання, перемішування, атака методом повного перебору, раундів ключ; опанувати методикою пошуку ключів при різних видах атак. **Вміти:** здійснювати вибір програм автоматичного шифрування інформації при її збереженні на дисках та відпрацювання практичних навичок їх застосування; проводити розшифрування файліві перевірку їх цифрових підписів.	**Тема 11: Методи криптоаналізу**	13
	Лекція 11 План лекції: 1. Поняття та зміст, типи криптоаналізу. 2. Методика пошуку ключа. 3. Види атак. 4. Оцінка ефективності криптографічногозахисту. **Література:** Основна: 1. Додаткова: 30. Інтернет-ресурси: 33, 37-39.	2
	Самостійна робота: Побудова хеш-функцій. Хеш-функції на основі блокових шифрів. Самостійні хеш-алгоритми. Електронний цифровий підпис. Робота з програмами шифрування на відкритому ключі. Освоєння програмних засобів електронного цифрового підпису.	7
	Лабораторна робота 21: Криптоаналіз План: 1. Атака методом повного перебору, раундів ключ. 2. Методика пошуку ключів при різних видах атак. 3. Використання криптографічного захисту електронної пошти.	2
	Лабораторна робота 22: Криптоаналіз План: 1. Пошук ключів при різних видах атак. 2. Використання криптографічного захисту електронної пошти.	2

1	2	3
Знати: види проявів шкідливого ПЗ, де шукати ознаки шкідливого програмного забезпечення **Вміти:** застосовувати методи захисту від шкідливих програм; здійснювати інсталяцію на робочій станції декількох сучасних антивіруснихпакетів; налаштовувати антивірусний монітор, антивірусний сканер; розклад використання антивірусного пакету.	**Тема 12: Захист від шкідливого програмного забезпечення**	13
	Лекція 12 План лекції: 1. Види проявів. 2. Ознаки шкідливого програмного забезпечення. 3. Методи захисту від шкідливих програм. 4. Оцінка ефективності криптографічного захисту. **Література:** Основна: 2, 8. Додаткова: 14, 23, 24, 25, 31. Інтернет-ресурси: 36.	2
	Самостійна робота: Оцінка ефективності сучасних антивірусних засобів. Тестовий вірус.	7
	Лабораторна робота 23: Основні ознаки присутності на комп'ютері шкідливих програм План 1. Вивчити налаштування браузера. 2. Визначити підозрілі процеси. 3. Дослідити елементи автозапуску. 4. Дослідити мережеву активність.	2
	Лабораторна робота 24: Визначення присутності на комп'ютері шкідливих програм План 1. Визначити підозрілі процеси. 2. Дослідити елементи автозапуску. 3. Дослідити мережеву активність.	2

1	2	3
Вміти: організовувати роботу по виявленню і блокуванню технічних каналів витоку інформації; налаштовувати парольний захист в електронному документообороті. **Вміти:** використовувати засоби для отримання віддаленого доступу та віддаленого керування робочими станціями у локальній мережі.	**Тема 13: Захист мережевого керування**	12
	Лекція 13 План лекції: 1. Основні принципи роботи протоколу SNMP. 2. Об'єднання SNMPv1 як засоби захисту SNMPv3. 3. Архітектура протоколу SNMPv3. 4. Обробка повідомлення в моделі USM. **Література:** Основна: 2, 8. Додаткова: 14, 31, 32.	2
	Самостійна робота: Модель обробки повідомлень і захисту користувача. Особливості захисту електронної корпоративної інформації.	6
	Лабораторна робота 25: Віддалений доступ до комп'ютера План: 1. Встановити на комп'ютери програмне забезпечення, яке складається з двох модулів: Модуля Admin (додаток-клієнт) та Модуль Host(додаток-сервер). 2. Підключитись до віддаленого комп'ютера та здійснити дистанційне управління згідно отриманого завдання.	2
	Лабораторна робота 26: Віддалений доступ до комп'ютера План: 1. Захиститися від проникнення до комп'ютера через механізми віддаленого доступу. 2. Організувати віртуальну приватну мережу.	2

1	2	3
Знати та розуміти: сутність та методику випровадження систем аналізу вразливостей та виявлення вторгнень провідних світових виробників **Вміти:** здійснювати інсталяцію, настройку та використання поштового серверу, антивірусного програмного забезпечення, відомих засобів розповсюдження спаму; проводити перевірку функціонування антивірусного програмного забезпечення.	**Тема 14: Перспективні напрями розвитку комплексів засобів захисту інформації**	12
	Лекція 14 План лекції: 1. Адаптивні комплекси засобів захисту інформації. 2. Методика зменшення ефективності атак та збільшення ефективності захисту за рахунок використання обчислювальних ресурсів порушника. 3. Сучасні системи аналізу вразливостей, виявлення вторгнень та їх використання. **Література:** Основна: 1, 2, 5, 10. Додаткова: 12, 13, 28.	2
	Самостійна робота: Механізми та засоби захисту програм та електронного документообігу від несанкціонованої модифікації та розповсюдження.Політика безпеки при опрацюванні електронної пошти. Захист електронної пошти від спаму. Визначення та класифікація спаму. Особливості „фішінгу”. Модель загроз від спаму. Методи розпізнавання спаму: чорні та білі списки, баєсовський підхід.	6
	Лабораторна робота 27: Налагодження параметрів безпеки засобів захисту від спаму. План: 1. Створити тестові віруси EICAR, CURE-EICAR та 2. SUSP-EICAR. 3. Протестувати антивірус за допомогою EICAR. 4. Вилікувати інфіковані файли.	2
	Лабораторна робота 28: Захист мобільного програмного забезпечення План: 1. Характеристика специфічних загроз. Особливості захисту мобільних програмних компонентів та системмобільних програмних агентів. 2. Задачі захисту мобільного програмного забезпечення та платформи його функціонування. 3. Вибір антивірусної програми. 4. Особливості системи безпеки COM/DCOM, ActiveX, Java, Framework, Flash Macromedia.	2
Всього за семестр		**180 /6**
Підсумковий контроль		**екзамен**

ІІІ. РЕКОМЕНДОВАНІ ДЖЕРЕЛА

Основні

1. *Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security = RSA Security's. Official Guide to Cryptography / Пер. с англ. под ред. А.И. Тихонова. 2-е изд., стереотип. Москва: Бином. 2007. 384с.*
2. *Вертузаєв М. С., Юрченко О. М. Захист інформації в комп'ютерних системах від несанкціонованого доступу : навч. посібник / за ред. С.Г. Лаптєва. Київ: Вид-во Європ. ун-ту, 2001.*
3. *Зубок М. І. Інформаційна безпека : навч. Посібник. Київ: КНТЕУ, 2009. 133 с.*
4. *Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навч. Посібник. Київ: Кондор, 2004. 384с.*
5. *Корнеев, И. К., Степанов Е. А. Защита информации в офисе : учебник. Москва: Проспект, 2007. 336с.*
6. Крегул Ю. І., Зубок М. І., Банк Р. О. Комерційна розвідка та внутрішня безпека на підприємстві : навч. посібник / за ред. Ю. І. Крегула. Київ: КНТЕУ, 2014. 176 с.
7. *Партыка Т. Л. Информационная безопасность : Учеб. Пособие. М. Форум, Инфра-М, 2007. – 368с. :*
8. *Прохода А. Н. Обеспечение интернет-безопасности : Практикум; Учеб. Пособие. М : Горячая линия - Телеком, 2007. – 180с.*
9. Пиріг С. О. Платіжні системи : навч. посібник. Київ: Центр учбової літератури, 2008. 240с.
10. Садердинов А. А., Трайнёв В. А., Федулов А. А. Информационная безопасность предприятия : учеб. Пособие. 4-е изд. Москва: Дашков и К, 2007. 336с.

Додаткові

11. Бедрій Я. І. Івах Р. М., Рощин В. О., Ємкало В. М. Цивільна оборона України : навч. Посібник. Київ: Кондор. 2011. 358 с.
12. Головко В. І., Мінченко А. В., Шарманська В. М. Фінансово-економічна діяльність підприємств: контроль, аналіз та безпека : навч. Посібник. Київ: Центр навчальної літератури, 2006. 448с.
13. Дубов Д. В., Дубова С. В. Основи електронного урядування : навч. Посібник. Київ: Центр навчальної літератури, 2006. 176 с.
14. Дудатьєв А. В., Войтович О. П., Каплун В. А. Захист комп’ютерних мереж. Теорія та практика: навч. посібник. Вінниця: ВНТУ, 2009. 219 с.

15. *Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. Посібник. Київ: КНТ, 2006. 280с.*
16. *Мазаракі А. А., Корольчук О. П., Мельник Т. М. та ін. Економічна безпека України в умовах глобалізаційних викликів : монографія / за заг. ред. А. А. Мазаракі. Київ: КНТЕУ, 2010. 718 с.*
17. *Ортинський В. Л., Керницький І. С., Живко З. Б. та ін. Економічна безпека підприємств, організацій та установ : навч. Посібник. Київ: Правова єдність, 2009. 544 с.*
18. Кавун С.В. Інформаційна безпека : навчальний посібник / С.В. Кавун, В.В. Носов, О.В. Манжай. – Харків : Вид. ХНЕУ, 2008. 352 с.
19. *Кислов Д. В. Інформаційні війни : монографія / Д. В. Кислов. К. : КНТЕУ, 2013. 300 с.*
20. Про державну таємницю: Закон України від 21 січня 1994 року №3855-XII. / База даних «Законодавство України. URL: http://zakon4.rada.gov.ua/laws/show/3855-12
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // Відомості Верховної Ради України (ВВР). 2011. № 32. Ст. 314.
22. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 р. №851-IV. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T030851.html
23. Про електронний цифровий підпис: Закон України від 22 травня 2003 р. №851-IV. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T030852.html
24. Про захист інформації в автоматизованих системах. Закон України від 05.07.94р. / *Відомості Верховної Ради України.* 1994.
25. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України (ВВР). – 1994. – № 31. – Ст. 286.
26. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // Відомості Верховної Ради України (ВВР). 2010. № 34. Ст. 481.
27. Про національну програму інформатизації: Закон України від 04.02.1998 №74/98 – ВР. / *Відомості Верховної Ради України*. 1998. №27-28. Ст. 181.
28. Про основні засади розвитку інформаційного суспільства в Україні 2007-2015 роки: Закон України від 09 січня 2007. / *ВідомостіВерховної Ради України*. 2007. № 12. Ст. 102.
29. Про основи національної безпеки України: Закон України від 19 червня 2003 р. / *Голос України*. 2003. №134.
30. Про порядок здійснення криптографічного захисту інформації в Україні: Указ президента України від 22 травня 1998 р. №505/98. URL: http://www.uapravo.net/akty/ministerstvo-main/akt9pprs7f.htm
31. Про положення про технічний захист інформації в Україні: Указ

президента України від 27 вересня 1999 р. №1229. / База даних «Законодавство України. URL: http://zakon4.rada.gov.ua/laws/show/1229/99

32. Соціальні мережі як інструмент взаємовпливу влади та громадянського суспільства : монографія / О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.; НАН України, Нац. б-ка України ім. В.І. Вернадського. К., 2014. 260 с.

3. Internet-ресурси

33. Анохин М. Блочные криптографические алгоритмы. URL: http://www.cryptography.ru/db/msg.html?mid=1162999&uri=node4.html
34. Безпека електронної комерції URL:: http://pistunovi.narod.ru/6_E_K.pdf. Назва з екрана.
35. Інформаційний портал Верховної Ради України URL:. : http://www.rada.gov.ua/. .
36. Основи інформаційної безпеки. Он-лайн курс URL: https://edx.prometheus.org.ua/courses/
37. Bruce Schneier “Self-Study Course in Block Cipher Cryptanalysis”, 2000. URL: http://www.counterpane.com/self-study.html
38. Francois-Xavier Standaert & others “Cryptanalysis of Block Ciphers: the Survey”, 2001, (повний огляд методів криптоаналізу). URL: http://logic.pdmi.ras.ru/~yura/crypto/01crypto.pdf.
39. Dave Rudolf “Development and Analysis of Block Ciphers and the DES System”, 2002. (Основи блочних шифрів). URL: http://www.cs.usask.ca/grads/dtr467/400.