МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ВІННИЦЬКИЙ ТОРГОВЕЛЬНО-КОНОМІЧНИЙ ІНСТИТУТ

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

Кафедра інформаційних систем та технологій

ЗАТВЕРДЖЕНО
Рішення вченої ради
31.03.2025
протокол № 05, п. 4

ВВЕДЕНО В ДІЮ
Наказ від 31.03.2025 № 67

КІБЕРБЕЗПЕКА / CYBERSECURITY

РОБОЧА ПРОГРАМА

Ступінь вищої освіти	«бакалавр» /	«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 2025

Розробник: Яремко Світлана, кандидат технічних наук, доцент

Гарант освітньої програми «Інформаційні технології у бізнесі» **–** Яремко Світлана, кандидат технічних наук, доцент

Обговорено та схвалено:
на засіданні кафедри економічної кібернетики та інформаційних систем від 10.03.2025, протокол № 03;
на засіданні вченої ради факультету економіки, менеджменту та права від 13.03.2025, протокол № 03

Рецензенти: Новицький Руслан, кандидат технічних наук
Богданова Лариса, директор МПВКП «Укрспецкомплекс»

Редактор: Фатєєва Т.
Комп'ютерна верстка: Шуляк Н.

Підп. до друку 21.04.2025 р. Формат 60x84/16. Папір офсетний
Друк ксероксний. Ум. друк. арк. 1,80.
Обл.-вид. арк. 1,30. Тираж 2. Зам. № 75.

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

І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Мета вивчення освітнього компонента.

Метою вивчення освітнього компонента є надання поглиблених знань з теорії та практики організації та забезпечення кібербезпеки для розв'язання професійних задач в процесі навчання та роботи за фахом.

Основними завданнями освітнього компонента є:

- загальні положення кібербезпеки;
- архітектура систем інформаційної безпеки;
- сучасні технології захисту інформації;
- організація ефективної системи безпеки комп'ютерних систем і мереж;
- управління інформаційною безпекою;
- організаційно-правові та технічні аспекти кібербезпеки;
- програмні засоби для захисту інформаційних процесів.

Вивчення освітнього компонента 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 освітнього компонента «Кібербезпека» та його місце в освітньому процесі.

Освітній компонент «Кібербезпека» для спеціальності 126 «Інформаційні системи та технології» викладається на другому курсі у другому семестрі загальним обсягом 180 годин / 6 кредитів.

Результатом вивчення освітнього компонента «Кібербезпека» є формування комплексу компетентностей:

- **загальні компетентності (ЗК):**

ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 2. Здатність застосовувати знання у практичних ситуаціях.

ЗК 3. Здатність до розуміння предметної області та професійної діяльності.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 6. Здатність до пошуку, оброблення та узагальнення інформації з різних джерел.

- **фахові компетентності:**

СК 1. Здатність аналізувати об'єкт проектування або функціонування та його предметну область.

СК 2. Здатність застосовувати стандарти в області інформаційних систем та технологій при розробці функціональних профілів, побудові та інтеграції систем, продуктів, сервісів і елементів інфраструктури організації.

КС 4. Здатність проектувати, розробляти та використовувати засоби реалізації інформаційних систем, технологій та інфокомунікацій (методичні, інформаційні, алгоритмічні, технічні, програмні та інші).

КС 5. Здатність оцінювати та враховувати економічні, соціальні, технологічні та екологічні фактори на всіх етапах життєвого циклу інфокомунікаційних систем.

КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.

КС 10. Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.

КС 12. Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет).

КС 10. Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.

КС 12. Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет).

КС 13. Здатність проводити обчислювальні експерименти, порівнювати результати експериментальних даних і отриманих рішень.

Програмні результати навчання здобувачів з освітнього компонента «Кібербезпека»:

ПР 3. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.

ПР 5. Аргументувати вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.

ПР 6. Демонструвати знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп’ютерних систем та середовищ з метою їх запровадження у професійній діяльності.

ПР 10. Розуміти і враховувати соціальні, екологічні, етичні, економічні аспекти, вимоги охорони праці, виробничої санітарії, пожежної безпеки та існуючих державних і закордонних стандартів під час формування технічних завдань та рішень

Міждисциплінарні зв'язки: робоча програма упорядкована відповідно до анотації освітньо-професійної програми підготовки бакалаврів, базується на вивченні таких нормативних освітніх компонент «Офісні комп’ютерні технології», «Комп’ютерні мережі», «Електронний бізнес», «Організація баз даних та знань».

Знання, отримані здобувачами вищої освіти під час вивчення освітнього компонента «Кібербезпека», є базою для опанування освітніх компонент циклу професійної підготовки, а також можуть бути застосовані під час проходження виробничої практики, підготовки курсових робіт за спеціальністю.

У результаті вивчення освітнього компонента здобувач вищої освіти зможе застосовувати набуті навички забезпечення кібербезпеки, роботи з електронними документами та цифровими джерелами, використання сучасного програмного забезпечення і мережевих технологій для захисту інформації та вирішення професійних задач у сфері інформаційної безпеки.

Критерії оцінювання результатів навчання

Критерієм успішного проходження здобувачем вищої освіти підсумкового оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання освітнього компоненту. Мінімальний пороговий рівень оцінки варто визначати за допомогою якісних критеріїв і трансформувати його в мінімальну позитивну оцінку використовуваної числової (рейтингової) шкали (табл. 1.1).

Таблиця 1 – Критерії оцінювання результатів навчання

Рівні компетентності	**За шкалою ДТЕУ**	**Критерії оцінювання**
1	2	3
Високий (дослідницький)	90-100	Має обґрунтовані та всебічні знання з освітнього компонента, 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 обгрунтуванням, 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 НПП виконує елементарні завдання.
	1-34	Ознайомлений з навчальним матеріалом на рівні розпізнавання та відтворення окремих фактів.

Для очної (денна, вечірня) форми навчання поточна робота оцінюється в 100 балів, підсумковий контроль (екзамен) оцінюється в 100 балів.

До екзамену допускаються всі здобувачі вищої освіти, які набрали за результатами поточної роботи протягом семестру 60 балів.

Результат підсумкового контролю (екзамен) з освітнього компоненту для здобувачів очної форми навчання визначається як середньоарифметична сума балів поточної роботи та екзамену.

Кращим здобувачам, які повністю виконали програму з освітнього компоненту, виявили активність в науково-дослідній роботі за відповідною тематикою, стали призерами студентських олімпіад, виступали на конференціях та за результатами поточної роботи набрали 90 і більше балів, науково-педагогічний працівник має право виставити результат екзамену без опитування (при усному екзамені) чи виконання екзаменаційного завдання (при письмовому екзамені).

Результат підсумкового контролю (екзамен) з освітнього компоненту для здобувачів заочної форми навчання оцінюється в 100 балів, відповідно до Положення про організацію освітнього процесу від 17.06.2024 № 08 зі змінами від 25.11.2024, протокол №12.

Згідно з цим же Положенням здобувач вищої освіти, який не погоджується з оцінкою, отриманою під час підсумкового контролю, має право в день оголошення результатів звернутися із заявою на ім’я директора з проханням апеляційного перегляду оцінки.

ОБСЯГ ОСВІТНЬОГО КОМПОНЕНТА В КРЕДИТАХ ТА ЙОГО РОЗПОДІЛ
(тематичний план)

Назва теми	Кількість годин				Форми контролю	Бальна оцінка
	Усього годин/ кредитів	з них				
		лекції	лабораторні заняття	самостійна робота здобувачів		
Тема 1. Основні положення теорії кібербезпеки	12	2	4	6	В, РПЗ, П	6
Тема 2. Поняття та зміст кіберзагроз	12	2	4	6	В, РПЗ, П	6
Тема 3. Методи зламу комп'ютерних мереж	12	2	4	6	В, РПЗ, П	6
Тема 4. Організаційно-правове забезпечення захисту інформації	12	2	4	6	В, РПЗ, П	6
Тема 5. Побудова систем захисту від загроз порушення конфіденційності інформації	12	2	4	6	В, РПЗ, П	6
Тема 6. Системи захисту цілісності інформаційних ресурсів	12	2	4	6	В, РПЗ, П	6
Тема 7. Методи та засоби забезпечення доступності інформації	12	2	4	6	В, РПЗ, П	6
Тема 8. Аналіз основних загроз інформаційних потоків підприємства	12	2	4	6	В, РПЗ, П	6
Тема 9. Організація інформаційної безпеки на підприємстві	7	2	2	3	В, РПЗ	3
Тема 10. Криптографічні методи захисту інформації	9	4	2	3	В, РПЗ	3
Тема 11. Методи криптоаналізу	14	4	4	6	В, РПЗ, П	6
Тема 12. Захист від шкідливого програмного забезпечення	14	4	4	6	В, РПЗ, П	6
Тема 13. Захист мережевого керування	14	4	4	6	В, РПЗ, П	6
Тема 14. Перспективні напрями розвитку комплексів засобів захисту інформації	2	2				
Індивідуальні завдання	**24**			**24**	**ІЗ**	**28**
Разом	**180/6**	**36**	**48**	**96**		**100**

Підсумковий контроль-екзамен	
Поточний контроль / критерії оцінювання	**Перелік умовних позначень форм контролю та оцінка їх у балах:** В – відповідь на практичних заняттях – 1 бал. РПЗ – розв'язання лабораторних завдань – 2 бали. УД – участь у дискусії – 1 бал. Т – тестування – 2 бали. Д – доповідь – 3 бали. П – презентація – 3 бали. ІЗ – індивідуальні завдання – 28 балів (курси на платформі Prometheus або на інших сервісах – 8 балів; участь у наукових заходах – 10 балів). **Загальна сума за поточну навчальну роботу (аудиторну та самостійну) за семестр – 100 балів.**

ІІ. ПРОГРАМА ОСВІТНЬОГО КОМПОНЕНТА

Зміст освітнього компонента (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 сфері інформаційної 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.

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 систем аутентифікації 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. Системи захисту цілісності інформаційних ресурсів

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. Методи та засоби забезпечення доступності інформаціїЗ

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. Захист 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.

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 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 засобів захисту інформації на підприємстві.

Організація на підприємстві групи влагоджування інцидентів комп'ютерної 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. 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. 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 ОСВІТНЬОГО КОМПОНЕНТА

Результати навчання	Навчальна діяльність	Робочий час здобувача, год.
1	2	3
Розуміти: поняття, зміст та роль інформаційної безпеки в сучасному світі; основні характеристики інформації: конфіденційність, цілісність, доступність, їх значення для безпеки; типи методів і способів захисту інформації, їх переваги та обмеження **Характеризувати:** сфери застосування та методи захисту інформації від загроз; застосовувати принципи та методи захисту інформації для забезпечення її безпеки.	**Тема 1. Основні положення теорії кібербезпеки** **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. **Рекомендовані джерела:** Основні: 2, 4, 5 Додаткові: 10, 14, 16 Інтернет-ресурси: 30, 32	2
	Самостійна робота здобувачів. 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.	6
	Лабораторне заняття №1 *Завдання до лабораторної роботи* 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
	Лабораторне заняття №2 *Завдання до лабораторної роботи* 1. Налаштувати двохфакторну авторизацію для захисту власної електронної пошти. 2. Налаштувати двохфакторну авторизацію для захисту акаунтів соціальних мереж.	2
Розуміти: інформаційні механізми впливу в сучасній політиці та роль інформаційних війн; основні класифікації загроз інформаційній	**Тема 2. Поняття та зміст кіберзагроз** **Лекція №2.** **План лекції** 1. Інформаційні механізми впливу в сучасній політиці. Інформаційні війни. 2. Основні класифікації загроз інформаційній безпеці.	2

1	2	3
безпеці; основні категорії кіберзагроз та їхнє значення для інформаційної безпеки. **Характеризувати:** типи загроз за засобами впливу та їх реалізацію в розподільчих системах; пояснювати специфіку інформаційних загроз у мережевих комунікаціях та засоби їхньої нейтралізації.	3. Загрози безпеки: за засобами впливу на систему, в розподільчих системах. 4. Інформаційні загрози мережевих комунікацій. **Рекомендовані джерела:** Основні: 1, 3, 6 Додаткові: 12, 13, 19 Інтернет-ресурси: 24, 27	
	Самостійна робота здобувачів. 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.	6
	Лабораторне заняття №3 *Завдання до лабораторної роботи* 1. Ознайомитись із класами захисту інформації згідно Оранжевої книги. 2. Визначити клас захисту для власної операційної системи.	2
	Лабораторне заняття №4 *Завдання до лабораторної роботи* 1. Перевірити вимоги гарантованості і документування. 2. Запропонувати способи виявлення атак.	2
Розуміти: історію розвитку методів зламу комп'ютерних мереж; сучасні методи зламу та їх еволюцію; принципи роботи сучасних методів зламу мереж.	**Тема 3. Методи зламу комп’ютерних мереж** **Лекція №3** **План лекції** 1. Історія методів зламу. 2. Вивчення сучасних методів. 3. Виконання атак. 4. Виявлення методів направлених та ненаправлених атак. **Рекомендовані джерела:** Основні: 4, 6, 8 Додаткові: 11, 12, 19 Інтернет-ресурси: 29, 31	2

1	2	3
Характеризувати: механізми реалізації атак та техніки їх виявлення; пояснювати різницю між направленими та ненаправленими атаками для оцінки загроз.	**Самостійна робота здобувачів.** Як зловмисник може використовувати фізичні засоби для отримання інформації або для її знищення. Використання економічного підходу при оптимізації засобів захисту.	6
	Лабораторне заняття №5 *Завдання до лабораторної роботи* 1. Визначити IP-адресу поштового сервера. 2. Відправити ping-пакети та просканувати адресний простір.	2
	Лабораторне заняття №6 *Завдання до лабораторної роботи* 1. Визначити IP-адресу веб-сервера інституту. 2. Визначите IP-адресу поштового сервера. 3. Дізнатися, які хости зараз знаходяться в режимі онлайн.	2
Розуміти: державно-правовий механізм забезпечення інформаційної безпеки; напрями державної інформаційної політики; законодавчу класифікацію видів інформації в Україні.	**Тема 4. Організаційно-правове забезпечення захисту інформації** **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. **Рекомендовані джерела:** Основні: 2, 5, 7 Додаткові: 13, 16, 18 Інтернет-ресурси: 21, 26	2
	Самостійна робота здобувачів. 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.	6

1	2	3
Характеризувати: нормативні акти, що регламентують технічний захист інформації; пояснювати принципи законодавчого регулювання захисту інформації та їх значення для безпеки.	**Лабораторне заняття №7** *Завдання до лабораторної роботи* 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
	Лабораторне заняття №8 *Завдання до лабораторної роботи* 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
Розуміти: причини та основні методи порушення конфіденційності інформації, їх вплив на безпеку; принципи роботи систем аутентифікації та ідентифікації; роль протоколу IPSec у забезпеченні конфіденційності та захисті інформації. **Характеризувати:** методи захисту від порушення конфіденційності та їх ефективність; пояснювати механізм розмежування доступу до інформації залежно від повноважень користувачів.	**Тема 5. Побудова систем захисту від загроз порушення конфіденційності інформації** **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. **Рекомендовані джерела:** Основні: 4, 5, 7 Додаткові: 12, 14, 16 Інтернет-ресурси: 30, 33	2
	Самостійна робота здобувачів. Захист авторських прав в інформаційних системах. Патентне та авторське право в Україні та світовій практиці. Захист елементів інформаційних систем патентами.	6

1	2	3
	Лабораторне заняття №9 *Завдання до лабораторної роботи* 1. Дослідження стійкості парольного захисту. 2. Багатофакторна авторизація.	2
	Лабораторне заняття №10 *Завдання до лабораторної роботи* 1. Реалізація та захист від флуд-атак. 2. Особливості керування доступом: потоковий, контроль висновку, контроль доступу; багаторівневий захист.	2
Розуміти: принципи забезпечення цілісності інформації та їхню важливість для безпеки даних; значення хеш-функцій та кодів перевірки автентичності для захисту цілісності інформації; методи та інструменти для забезпечення цілісності інформації.	**Тема 6. Системи захисту цілісності інформаційних ресурсів** **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. **Рекомендовані джерела:** Основні: 4, 5, 7 Додаткові: 12, 14, 16 Інтернет-ресурси: 30, 32	2
Характеризувати: роботу хеш-функцій і їх застосування для перевірки цілісності даних; пояснювати роль ідентифікації програм і захисту авторських прав у контексті кібербезпеки.	**Самостійна робота здобувачів.**: 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.	6

1	2	3
	Лабораторне заняття №11 *Завдання до лабораторної роботи* 1. Дослідити проблеми безпеки даних, що передаються мережевим трафіком. 2. Виявити загрози безпеці мережевих даних.	2
	Лабораторне заняття №12 *Завдання до лабораторної роботи* 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
Розуміти: структуру системи захисту від загроз порушення доступності та її компоненти; принципи резервного копіювання інформації та їх значення для безперервності доступу до даних. **Характеризувати:** аналізувати методи резервного копіювання для запобігання втрати даних; пояснювати необхідність побудови надійних систем захисту від загроз порушення стабільної роботи інформаційних ресурсів.	**Тема 7. Методи та засоби забезпечення доступності інформації** **Лекція №7** **План лекції** 1. Структура системи захисту від загроз порушення доступності. 2. Дублювання шлюзів і міжмережевих екранів. 3. Резервне копіювання інформації. **Рекомендовані джерела:** Основні: 4, 6, 8 Додаткові: 12, 14, 15 Інтернет-ресурси: 29, 31	2
	Самостійна робота здобувачів. 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.	6

1	2	3
	Лабораторне заняття №13 *Завдання до лабораторної роботи* 1. Установити Certificate Services. 2. Створити сертифікат, додати центр сертифікації (Certificate Authority) в список довірених. 3. За допомогою сертифіката захистити створений віртуальний каталог.	2
	Лабораторне заняття №14 *Завдання до лабораторної роботи* 1. Створити сертифікат, додати центр сертифікації (Certificate Authority) в список довірених. 2. За допомогою сертифіката захистити створений віртуальний каталог.	2
Розуміти: структуру системи захисту від загроз порушення доступності та її компоненти; принципи резервного копіювання інформації та їх значення для безперервності доступу до даних. **Характеризувати:** методи та засоби для захисту електронних документів підприємства.	**Тема 8. Аналіз основних загроз інформаційних потоків підприємства** **Лекція №8** **План лекції** 4. Аналіз основних загроз інформаційних потоків підприємства 5. Безпека діловодства та конфіденційної інформації. 6. Методи та засоби захисту інформаційних потоків підприємства. **Рекомендовані джерела:** Основні: 1, 6, 7 Додаткові: 9, 10, 15 Інтернет-ресурси: 21, 30	2
	Самостійна робота здобувачів. Спеціальне діловодство на підприємстві. Особливості захисту офісних електронних документів від несанкціонованого доступу, несанкціонованої модифікації та розповсюдження.	6

1	2	3
	Лабораторне заняття №15 *Завдання до лабораторної роботи* 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
	Лабораторне заняття №16 *Завдання до лабораторної роботи* 1. При необхідності модифікувати структуру. шаблону для опису політики кібербезпеки. 2. Розробити політику кібербезпеки з урахуванням специфіки діяльності та планів розвитку підприємства (підрозділу).	2
Розуміти: організацію політики безпеки на підприємстві; міжнародні стандарти управління інформаційною безпекою; основи організації ефективної системи безпеки підприємства.	**Тема 9. Організація інформаційної безпеки на підприємстві** **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. **Рекомендовані джерела:** Основні: 5, 6, 7 Додаткові: 9, 10, 15 Інтернет-ресурси: 21, 30	2

1	2	3
Характеризувати: принципи оптимального використання парольного захисту інформації; пояснювати необхідність побудови надійної системи безпеки для захисту інформаційних ресурсів підприємства.	**Самостійна робота здобувачів.** Обмеження доступу до інформації в інтересах слідства та судочинства. Особливості захисту інформації під час розслідування кримінальних справ.	3
	Лабораторне заняття №17 *Завдання до лабораторної роботи* 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), 4. Виділити потоки з інформацією, що потребує захисту, визначити її статус (комерційна таємниця, службова інформація, фінансова інформація, лише для внутрішнього використання, загальнодоступна тощо). 5. Побудувати таблицю розмежування доступу для різних категорій працівників або відділів. 6. Розробити політику кібербезпеки верхнього рівня підприємства.	2
Розуміти: криптографічні методи захисту інформації; розвиток технологічних засобів криптографії; загальну класифікацію класичних шифрів. **Характеризувати:** принципи роботи блочних шифрів та асиметричного шифрування; пояснювати важливість криптографії як засобу захисту інформації у сучасних інформаційних системах.	**Тема 10. Криптографічні методи захисту інформації** **Лекція №10** **План лекції** 1. Криптографічні методи захисту інформації. 2. Розвиток технологічних засобів криптографії. **Лекція №11** **План лекції** 1. Загальна класифікація класичних шифрів. 2. Блочні шифри. Асиметричне шифрування. **Рекомендовані джерела:** Основні: 4, 5, 7 Додаткові: 12, 14, 16 Інтернет-ресурси: 30, 32	2 2

1	2	3
	Самостійна робота здобувачів. Реалізація криптографічних методів захисту інформації. Управління ключами. Шифрування потоків даних і повідомлень великого обсягу. Використання «блукаючих ключів». Шифрування, завадостійке кодування і стиснення інформації.	3
	Лабораторне заняття №18 *Завдання до лабораторної роботи* 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
Розуміти: поняття, зміст та типи криптоаналізу; методику пошуку ключа в криптографічних системах; різні види атак на криптографічні системи. **Характеризувати:** методи оцінки ефективності криптографічного захисту; пояснювати важливість криптоаналізу для забезпечення надійності криптографічного захисту інформації.	**Тема 11: Методи криптоаналізу** **Лекція №12** **План лекції** 1. Поняття та зміст, типи криптоаналізу. 2. Методика пошуку ключа. **Лекція №13** 1. Види атак. 2. Оцінка ефективності криптографічного захисту. **Рекомендовані джерела:** Основні: 4, 5, 7 Додаткові: 12, 14, 16 Інтернет-ресурси: 30, 32	2 2
	Самостійна робота здобувачів. 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.	6

1	2	3
	Лабораторне заняття №19 *Завдання до лабораторної роботи* 1. Атака методом повного перебору, раундів ключ. 2. Методика пошуку ключів при різних видах атак. 3. Використання криптографічного захисту електронної пошти.	2
	Лабораторне заняття №20 *Завдання до лабораторної роботи* 1. Пошук ключів при різних видах атак. 2. Використання криптографічного захисту електронної пошти.	2
Розуміти: види проявів шкідливого програмного забезпечення; ознаки шкідливого ПЗ та його потенційні загрози; методи захисту від шкідливих програм. **Характеризувати:** методи оцінки ефективності захисту від шкідливого ПЗ; пояснювати необхідність використання ефективних засобів захисту для запобігання шкідливому впливу програм на інформаційну систему. .	**Тема 12. Захист від шкідливого програмного забезпечення** **Лекція №14** **План лекції** 1. Види проявів. 2. Ознаки шкідливого програмного забезпечення.	2
	Лекція №15 **План лекції** 1. Методи захисту від шкідливих програм. 2. Оцінка ефективності криптографічного захисту. **Рекомендовані джерела:** Основні: 4, 6, 8 Додаткові: 12, 14, 19 Інтернет-ресурси: 29, 31	2
	Самостійна робота здобувачів. Оцінка ефективності сучасних антивірусних засобів. Тестовий вірус.	6
	Лабораторне заняття №21 *Завдання до лабораторної роботи* 1. Вивчити налаштування браузера. 2. Визначити підозрілі процеси. 3. Дослідити елементи автозапуску. 4. Дослідити мережеву активність.	2
	Лабораторне заняття №22 *Завдання до лабораторної роботи* 1. Вивчити налаштування операційної системи. 2. Визначити підозрілі процеси. 3. Дослідити елементи автозапуску. 4. Дослідити мережеву активність.	2

1	2	3
Розуміти: основні принципи роботи протоколу SNMP; архітектуру протоколу SNMPv3 та її значення для безпеки мережевого керування; обробку повідомлень у моделі USM (User-based Security Model) протоколу SNMPv3. **Характеризувати:** об'єднання SNMPv1 як засіб захисту SNMPv3; пояснювати важливість використання безпечних версій протоколу SNMP для захисту мережевого керування.	**Тема 13. Захист мережевого керування** **Лекція №16** **План лекції** 1. Основні принципи роботи протоколу SNMP. 2. Об'єднання SNMPv1 як засоби захисту SNMPv3. **Лекція №17** **План лекції** 1. Архітектура протоколу SNMPv3. 2. Обробка повідомлення в моделі USM. **Рекомендовані джерела:** Основні: 4, 6, 8 Додаткові: 12, 14, 15 Інтернет-ресурси: 29, 31	2 2
	Самостійна робота здобувачів. Модель обробки повідомлень і захисту користувача. Особливості захисту електронної корпоративної інформації.	6
	Лабораторне заняття №23 *Завдання до лабораторної роботи* 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
	Лабораторне заняття №24 *Завдання до лабораторної роботи* 1. Захиститися від проникнення до комп'ютера через механізми віддаленого доступу. 2. Організувати віртуальну приватну мережу.	2
Розуміти: адаптивні комплекси засобів захисту інформації; сучасні системи аналізу вразливостей та виявлення вторгнень; перспективи та напрямки вдосконалення організаційно-технічних рішень у розробці політики інформаційної безпеки.	**Тема 14. Перспективні напрями розвитку комплексів засобів захисту інформації** **Лекція №18** **План лекції** 1. Адаптивні комплекси засобів захисту інформації. 2. Методика зменшення ефективності атак та збільшення ефективності захисту за рахунок використання обчислювальних ресурсів порушника.	2

1	2	3
Характеризувати: зменшення ефективності атак та підвищення ефективності захисту за рахунок використання обчислювальних ресурсів порушника; пояснювати важливість адаптації до нових загроз та технологічних змін.	3. Сучасні системи аналізу вразливостей, виявлення вторгнень та їх використання. 4. Урахування перспектив та напрямків вдосконалення організаційно-технічних рішень в процесі розробки політики інформаційної безпеки. **Рекомендовані джерела:** Основні: 1, 3, 5 Додаткові: 10, 13, 17 Інтернет-ресурси: 24, 28	
Індивідуальне завдання		**24**
Всього		**180 / 6**

ІІІ. РЕКОМЕНДОВАНІ ДЖЕРЕЛА

Основні

1. Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. Кібербезпека України: аналіз поточного стану. Ukrainian Information Security Research Journal. 2019. №3(21). С. 642–646.
2. Сопілко І.М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. Юридичний вісник Повітряне і космічне право. Київ: НАУ, 2021. № 2(59). С. [номер сторінки не вказаний].
3. Трофименко О. Моніторинг стану кібербезпеки в Україні. Правове життя сучасної України: матер. міжнар. наук.-практ. конф., 17 травня 2019 р., Т. 1. Одеса: Видавничий дім «Гельветика», 2019. С. 642–646.
4. Schatz D., Bashroush R., Wall J. Towards a More Representative Definition of Cyber Security. Journal of Digital Forensics, Security and Law. 2017. № 2. С. 54-74. DOI: https://doi.org/10.15394/jdfsl.2017.1476.
5. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий електронний журнал. 2020. № 2. С. 200-203.
6. Кузьменко О., Маклюк О., Чернишова О. Кібербезпека бізнесу під час війни. Ukrainian Information Security Research Journal. 2022. №44. DOI: https://doi.org/10.32782/2524-0072/2022-44-21.
7. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. Товари і ринки. 2022. № 3. С. 47–59.
8. Вишнівський В. В., Пампуха А. І. Кібербезпека в Україні. Цифрова трансформація кібербезпек: науково-практична інтернет-конференція, 20 квітня 2022, Державний університет телекомунікацій Навчально-наукового інституту захисту інформації. Київ, 2022. С. 31–33.

Додаткові

9. Трансформація менеджменту бізнес-організацій: сучасні тренди та виклики [Електронний ресурс] : монографія / за заг. ред. Сагайдака М.П., Соболєвої Т.О. Київ: КНЕУ, 2021. 378 с.
10. Кіндзерський Ю.В. Кібербезпека та становлення цифрової економіки: проблеми взаємозв’язку. Економічний вісник Дніпровської політехники. 2020. №3(71).
11. Mat B., Pero S., Wahid R., Sule B. Cybersecurity and Digital Economy in Malaysia: Trusted Law for Customer and Enterprise Protection. International Journal of Innovative Technology and Exploring Engineering, 2019. www.ijitee.org/wp-content/uploads/papers/v8i8s3/H10610688S319.pdf (Дата звернення 21.07.2020).

12. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія. / С. Ф. Гончар. Київ, 2019. 175 с.

13. Грановський М. В. Державна політика у сфері запобігання та протидії кібернетичним загрозам – досвід Республіки Польща. Теорія та практика державного управління. 2019. Вип. 4. С. 212–220.

14. Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія. / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька. Житомир, 2019. 279 с.

15. Комова С.С. Кібербезпека в цифровій економіці. Матеріали XVI Всеукраїнської студентської науково-технічної конференції «Сталий розвиток міст». Частина 3. Харків: ХНУМГ ім. О.М. Бекетова, 2023.

16. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. К.: Видавничий дім «Кондор», 2019. 272 с.

17. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. Державний торговельно-економічний університет. 2022.

18. Дергачова Г. М., Колешня Я. О. Цифрова трансформація бізнесу: сутність, ознаки, вимоги та технології. Економічний вісник НТУУ "КПІ". 2020. № 17. С. 280-290.

19. Гуцалюк М. В. Окремі аспекти боротьби з організованою кіберзлочинністю. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук.-практ. конф. (м. Київ, 4 квітня 2019 р.). Київ: Нац. акад. СБУ, 2019. С. 199-201.

Internet-ресурси

20. Впровадження європейської кібербезпеки: загальний огляд. ISACA. [Електронний ресурс]. Режим доступу: https://www.isaca.org/Knowledge-Center/Research/Documents/European-CybersecurityImplementation-Overview_res_Ukr_1215.pdf.

21. Державне агентство з електронного врядування України. [Електронний ресурс]. Режим доступу: https://www.e.gov.ua/ua.

22. Завдання Держспецзв’язку. [Електронний ресурс]. Режим доступу: http:// www.dsszzi.gov.ua/ dsszzi/ control/uk/publish/article?art_id=89831& cat_id=89828.

23. Офіційний сайт кіберполіції України: про підрозділ. [Електронний ресурс]. Режим доступу: https:// cyberpolice.gov.ua/contacts/.

24. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері. Київ, 28 с., 2019. [Електронний ресурс]. Режим доступу: https:// geostrategy.org.ua/ua/analitika/item/1565-cooperation-ukraine-nato

25. У Держспецзв’язку відбулося відкриття найпотужнішого в ЄС Центру реагування на кіберзагрози. [Електронний ресурс]. Режим доступу: http:// www.dsszzi.gov.ua/dsszzi/control/uk/publish/article ?art_id=286338&cat_id=284576.

26. Функції захисту персональних даних покладено на уповноваженого. [Електронний ресурс]. Режим доступу: http:// www.ombudsman.gov.ua/ ua/ page/ zpd/.

27. R. Moody, "Which countries have the worst (and best) cybersecurity?" [Електронний ресурс]. Режим доступу: https://www.comparitech.com/blog/vpnprivacy/cybersecurity-by-country/. [16]. National Strategies. [Електронний ресурс]. Режим доступу: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx. [17].

28. Security Council Calls on Member States to Address Threats against Critical Infrastructure, Unanimously Adopting Resolution 2341 (2017), United Nations. [Електронний ресурс]. Режим доступу: https://www. un.org/press/en/2017/sc12714.doc.htm.

29. 2020 Data Breach Investigations Report. Verizon. 2020. URL: https://enterprise.verizon.com/ resources/reports/2020-data-breach-investigationsreport.pdf.

30. Fasulo P. Cybersecurity vs Information Security: What's the difference? Security Scorecard. 2020. URL: https://securityscorecard.com/blog/ information-security-versus-cybersecurity.

31. Fruhlinger J. What is information security? Definition, principles, and jobs. CSO United States. 2020. URL: https://www.csoonline.com/article /3513899/what-is-information-security-definitionprinciples-and-jobs.html.

32. Information Security and Cyber Security: The Key Differences and Similarities. Simplilearn. 2021. URL: https://www.simplilearn.com/ information-security-vs-cyber-security-article.

33. Irwin L. What's the difference between information security and cyber security? IT Governance. 2020. URL: https://www.itgovernance.eu/ blog/en/whats-the-difference-between-informationsecurity-and-cyber-security.

34. It Security vs Cyber Security - What is the Difference? Logsign. 2020. URL: https://www.logsign.com/blog/it-security-vs-cybersecurity-what-is-the-difference/.

35. Reimers K., Andersson D. Post-secondary education network security: the end user challenge and evolving threats. ICERI2017 Proceedings. 2017. Pp. 1787-1796. DOI: https://doi.org/ 10.21125/iceri.2017.0554