ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«КИЇВСЬКИЙ ФАХОВИЙ КОЛЕДЖ МІСЬКОГО ГОСПОДАРСТВА ТАВРІЙСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ В. І. ВЕРНАДСЬКОГО»

Циклова комісія комп'ютерно-інтегрованих технологій

ЗАТВЕРДЖУЮ
Заступник директора коледжу з навчально-виховної роботи
_____ ЛюдмилаПУСТОВОЙТ
«30» серпня 2023року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ВНПП03.04.01 Захист інформації та безпека ПК мереж

підготовки фахового молодшого бакалавра
освітньо-професійної програми Обслуговування комп'ютерних систем і мереж
спеціальності 123 Комп'ютерна інженерія

Відділення екології, комп'ютерних систем та автоматизації

Київ – 2023 рік

Робоча програма з дисципліни «Захист інформації та безпека ПК мереж» для підготовки молодших спеціалістів І-ІІ рівня акредитації для студентів IV курсу галузі підготовки: «Інформатика та обчислювальна техніка»

спеціальності: 123 «Обслуговування комп'ютерних систем і мереж»

Розробники:
Катерина ЛУКАШЕНКО – викладач, категорія - спеціаліст
Тетяна СИДОРЕНКО – викладач, категорія - спеціаліст

Робочу програму схвалено:
на засіданні циклової комісії комп'ютерно-інтегрованих технологій
Протокол № 1 від «28» серпня 2023 року

Голова циклової комісії: Людмила ГЛУШКО

Розглянуто і рекомендовано до затвердження
навчально-методичною радою коледжу
Протокол № 1 від «30» серпня 2023 року

Голова НМР: Аліна ОДИНЕЦЬ

ЗМІСТ

1 ПОЯСНЮВАЛЬНА ЗАПИСКА 4
2 НАВЧАЛЬНО-ТЕМАТИЧНИЙ ПЛАН 8
3 КАЛЕНДАРНО-ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ 9
4 ТЕМИ І ПЛАНИ ЛЕКЦІЙНИХ ЗАНЯТЬ 10
5 ТЕМИ І ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ 13
6 ТЕМИ І ПИТАННЯ ДО САМОСТІЙНОЇ РОБОТИ СТУДЕНТА 14
СИСТЕМА ПОТОЧНОГО І ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ 17
ПИТАННЯ ТА ЗАВДАННЯ ДО ЗАЛІКУ 17
КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ 20
РЕКОМЕНДОВАНА ЛІТЕРАТУРА 22
ДОДАТКИ 24

1 ПОЯСНЮВАЛЬНА ЗАПИСКА

На сьогоднішній день ми спостерігаємо, що сучасні технології використовуються в усіх сферах життя. В електронному вигляді зберігається маса важливої інформації. Дана дисципліна допоможе вивчити шляхи захисту інформації в комп'ютерних мережах.

Мета дисципліни – ознайомлення студентів з основним засобами захисту інформації в комп'ютерних системах і розподілених комп'ютерних (інформаційно-комунікаційних) системах від зовнішніх та внутрішніх загроз.

Завдання дисципліни – ознайомлення з фаховою термінологією, розглянути основні загрози, які можуть виникнути під час роботи з ПК. Опанування програмних засобів для захисту інформації.

Процес вивчення дисципліни ВНПП03.04.01 «Захист інформації та безпека ПК мереж» спрямований на формування елементів наступних компетентностей:

а) загальні компетентності (ЗК):

КЗ1. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

КЗ2. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ4. Здатність спілкуватися державною мовою як усно, так і письмово.

КЗ5. Здатність спілкуватися іноземною мовою.

КЗ6. Здатність здійснювати професійну діяльність згідно з вимогами санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки.

КЗ7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел та практичного її застосування.

КЗ8. Здатність вчитися і бути сучасно навченим.

б) спеціальні (фахові) компетентності (СК):

КФ1. Здатність застосовувати законодавчу та нормативно- правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності в галузі інформаційних технологій.

КФ2. Здатність використовувати професійно-орієнтовані знання в галузі математики при розв’язанні прикладних і наукових завдань в області комп’ютерної інженерії.

КФ3. Розуміння закономірностей випадкових явищ і вміння застосовувати ймовірносно-статистичні методи для вирішення професійних завдань.

КФ7. Здатність використовувати професійно-орієнтовані знання і практичні навички з дисциплін циклу професійної та практичної підготовки для проектування, побудови та обслуговування сучасних комп’ютерних мереж різного виду та призначення.

КФ10. Здатність здійснювати вибір, розробляти, розгортати, інтегрувати, діагностувати, адмініструвати та експлуатувати комп’ютерні системи та мережі, мережеві ресурси, сервіси та інфраструктуру організації.

КФ11. Здатність до ділових комунікацій у професійній сфері, знання основ ділового спілкування, навички роботи в команді.

КФ12. Здатність здійснювати організацію робочих місць з урахуванням вимог безпеки життєдіяльності і охорони праці, їх технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

КФ13. Здатність оцінювати і враховувати економічні, соціальні, технологічні та екологічні чинники, що впливають на сферу професійної діяльності.

КФ14. Здатність аргументувати вибір методів розв’язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати прийняті рішення.

Очікувані результати навчання.

РН1. Знати способи аналізу, синтезу та подальшого сучасного навчання. Вміти проводити аналіз інформації, приймати обґрунтовані рішення, вміти придбати сучасні знання. Встановлювати відповідні зв’язки для досягнення цілей. Нести відповідальність за своєчасне набуття сучасних знань.

РН2. Мати спеціалізовані концептуальні знання, набуті у процесі навчання. Вміти розв’язувати складні задачі і проблеми, які виникають у професійній діяльності. Зрозуміле і недвозначне донесення власних висновків, знань та пояснень, що їх обґрунтовують, до фахівців та нефахівців. Відповідати за прийняття рішень у складних умовах.

РН3. Мати глибокі знання із структури професійної діяльності. Вміти здійснювати професійну діяльність, що потребує оновлення та інтеграції знань. Здатність ефективно формувати комунікаційну стратегію у професійній діяльності. Нести відповідальність за професійний розвиток, здатність до подальшого професійного навчання з високим рівнем автономності.

РН4. Знати види та способи адаптації, принципи дії в новій ситуації. Вміти застосувати засоби саморегуляції, вміти пристосовуватися до нових ситуацій (обставин) життя та діяльності. Встановлювати відповідні зв’язки для досягнення результату. Нести відповідальність своєчасне використання методів саморегуляції.

РН5. Знати тактики та стратегії спілкування, закони та способи комунікативної поведінки. Вміти приймати обґрунтоване рішення, обирати

способи та стратегії спілкування для забезпечення ефективної командної роботи. Нести відповідальність за вибір та тактику способу комунікації.

РН6. Мати досконалі знання державної мови та базові знання іноземної мови. Вміти застосовувати знання державної мові, як усно так і письмово, вміти спілкуватись іноземною мовою. Використовувати при фаховому та діловому спілкуванні та при підготовці документів державну мову. Використовувати іноземну мову у професійній діяльності.

РН7. Знати свої соціальні та громадські права та обов'язки. Формувати свою громадянську свідомість, вміти діяти відповідно до неї. Здатність донести свою громадську та соціальну позицію. Відповідати за свою громадянську позицію та діяльність.

РН8. Знати проблеми збереження навколишнього середовища та шляхи його збереження. Вміти формувати вимоги до себе та оточуючих щодо збереження навколишнього середовища. Нести відповідальність щодо виконання заходів збереження навколишнього середовища в рамках своєї компетенції.

РН11. Володіти базовими знаннями фундаментальних наук, в обсязі, необхідному для освоєння навчальних дисциплін професійної підготовки.

РН12. Вміти застосовувати базові знання стандартів в області інформаційних технологій при розробці та впровадженні інформаційних систем і технологій

РН13. Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних.

РН14. Володіти навиками аналізу навчальної і спеціальної літератури, нормативних положень, технічної документації для вирішення проблем, що виникають у професійній діяльності.

РН43. Вміти економічно мислити, орієнтуватися у конкретних виробничих ситуаціях, аналізувати показники виробничої діяльності підприємства.

РН44. Вміти здійснювати контроль за дотриманням норм охорони праці, техніки безпеки, екологічної та протипожежної безпеки, та умов безпеки життєдіяльності.

РН45. Практично володіти рідною та однією з іноземних мов в обсязі тематики, зумовленої професійними потребами.

РН46. Використовувати відповідну термінологію у власних дослідженнях та професійній діяльності державною мовою та/або іноземною; спілкуватися в діалоговому режимі в галузі професійної діяльності; вміти презентувати результати власних досліджень та описувати їх у фахових публікаціях, використовуючи сучасні інформаційні та комунікативні технології.

РН48. Вдосконалювати професійний та особистісний розвиток протягом усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

РН49. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

РН50. Дотримуватися етичних норм, враховуючи авторське право та норми академічної доброчесності при проведенні досліджень, розробці програмних продуктів, проектів, презентацій результатів роботи.

2 НАВЧАЛЬНО-ТЕМАТИЧНИЙ ПЛАН

№	Назва розділу	Кількість годин			
		Всього	Лекції	Прак.	СРС
1	Загальні поняття та положення із захисту інформації	30	8	4	20
2	Комплексна система захисту інформації	30	6	6	16
Всього		60	14	10	36

3 КАЛЕНДАРНО-ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№	Назва розділу, теми, заняття	Кількість годин		
		Л.	**Пр.**	**С.р.**
Розділ І. Загальні поняття та положення із захисту інформації				
	Тема 1.1. Концепція захисту інформації та інформаційних технологій			
1.	Концепція захисту інформації та інформаційних технологій. Категорії комп'ютерної безпеки	2		5
2.	Правове регулювання обігу та захисту інформації	2		5
3.	Основні види загроз конфіденційності інформації	2		5
	Тема 1.2 Основні методи захисту ПЗ			
4.	Основні методи захисту ПЗ: від вірусів, від незадекларованих можливостей ПЗ (закладок)	2		5
5.	ПР №1. Вивчення перших методів шифрування інформації		2	
6.	ПР №2. Огляд складових інформаційної безпеки		2	
	Разом по розділу	8	4	20
Розділ ІІ. Комплексна система захисту інформації				
	Тема 1.3 Організація системи захисту інформації			
7.	Організація системи захисту інформації. Політика безпеки	2		5
8.	ПР №3. Використання кейлогерів для збереження інформації.		2	
9.	Електронний цифровий підпис	2		5
10.	ПР №4. Генерування і використання електронного цифрового підпису для реалізації захисту файлів користувача.		2	
	Тема 1.4 Безпека Інтернет-застосувань			
11.	Захист інформації шляхом перетворення. Криптографічні вимоги до захисту інформації. Особливості стеку мережевих протоколів	2		6
12.	ЛР №5. Робота з криптографічними засобами шифрування інформації		2	
	Разом по розділу	**6**	**6**	**16**
	Разом по курсу	**14**	**10**	**36**

4 ТЕМИ І ПЛАНИ ЛЕКЦІЙНИХ ЗАНЯТЬ

№	Назва теми	Кількість годин
Розділ І. Основи захисту інформації		
	Тема 1.1. Концепція захисту інформації та інформаційних технологій.	
Л-1	*Концепція захисту інформації та інформаційних технологій. Категорії комп'ютерної безпеки* План: 1. Категорії комп'ютерної безпеки. Огляд найбільш розповсюджених методів комп'ютерного проникнення («злому») 2. Сучасна ситуація в області інформаційної безпеки. Роль та стан захисту інформації в сучасному світі. 3. Концепція і концептуальна модель інформаційної безпеки. 4. Класифікація загроз безпеці комп'ютерних систем. Загрози даним. Рівні захисту даних. Протидія загрозам. *Література:Гапак О. М. с. 5-18*	2
Л-2	*Правове регулювання обігу та захисту інформації* План 1. Захист інформації на законодавчому рівні. 2. Персональні дані. 3. Володільці та розпорядники персональних даних. 4. Згода на оброку персональних даних. 5. Дотримання безпеки обробки персональних даних. *Література: Бем М. В., с. 10-20*	2
Л-3	*Основні види загроз конфіденційності інформації* План: 1. Проблеми безпеки мереж. Джерела загроз в мережах. Види загроз і протидія їм. 2. Атаки на мережеві системи: на апаратну частину, файловий сервер, на пароль, на канал телефонного зв'язку. 3. Напрямки (види) забезпечення інформаційної безпеки. Законодавча база України в цій галузі. 4. Основні міри, способи та засоби захисту інформації в ПК, серверах, локальних мережах під час зберігання та передачі по телекомунікаційних каналах. *Література:Гапак О. М. с. 14-18, 24-27.*	2
	Тема 1.2 Основні методи захисту ПЗ	
Л-4	*Основні методи захисту ПЗ: від вірусів, від незадекларованих можливостей ПЗ (закладок)*	2

№	Назва теми	Кількість годин
	План: 1. Руйнуючі програмні засоби. Програми з потенційно шкідливим впливом та їх властивості. Основні класи руйнуючих програм. 2. Поняття комп'ютерний вірус. Класифікація комп'ютерних вірусів. Засоби розповсюдження 3. Вірус «троян». Модель вірусу та модель «трояна». 4. Програми «кілогери» – «клавіатурні шпигуни», визначення та класифікація. Налагодження антикілогерів. *Література:Гапак О. М. с.14-18*	
Розділ ІІ. Комплексна система захисту інформації		
	Тема 1.3 Організація системи захисту інформації	
Л-5	*Організація системи захисту інформації. Політика безпеки.* План: 1. Політика безпеки. Методи захисту даних. Програми тестування та діагностики. 2. Оптимізація дисків. Методи стискання та резервного зберігання інформації. 3. Ідентифікація і аутентифікація користувачів. Поняття про ідентифікацію користувача та її особливості. 4. Основні принципи та методи аутентифікації. *Література:Гапак О. М. с. 53-61*	2
Л-6	*Електронний цифровий підпис* План: 1. Проблема аутентифікації даних і електронний цифровий підпис 2. Хеш-функція 3. Алгоритми електронного цифрового підпису *Література:Гапак О. М. с.146-151*	2
	Тема 1.4 Безпека Інтернет-застосувань	
Л-7	*Захист інформації шляхом перетворення. Криптографічні вимоги до захисту інформації. Особливості стеку мережевих протоколів* План: 1. Криптографічні вимоги до захисту інформації 2. Вразливі місця з точки зору безпеки даних в стеку мережевих протоколів. 3. Протоколи безпеки комп'ютерних мереж (IPSec, SSL, HTTPS) 4. Використання брандмауерів та мережевих екранів.	2

№	Назва теми	Кількість годин
	Література:Гапак О. М. с. 65-75	
	Всього годин	**14**

5 ТЕМИ І ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ

№	Назва теми	Кількість годин
Розділ І. Основи захисту інформації		
	Тема 1.2. Основні методи захисту ПЗ	
1	*ПР №1. Вивчення перших методів шифрування інформації.* План: 1. Зашифрувати інформацію за допомогою шифра Цезаря. 2. Зашифрувати інформацію за допомогою шифру з використання кодового слова. 3. Зашифрувати інформацію за допомогою шифру з простої заміни. *Література:Гапак О. М. с. 77-87*	2
2	*ПР №2. Огляд складових інформаційної безпеки.* План: 1. Розглянути наведені ситуації загрози ІБ. 2. Прокласифікувати ситуації за ознаками. *Література: Гапак О. М. с.7-14*	2
Розділ ІІ. Комплексна система захисту інформації		
	Тема 1.3 Організація системи захисту інформації	
3	*ПР №3. Використання кейлогерів для збереження інформації.* План: 1. Укажіть для чого використовують Keylogger на підприємствах. 2. Розгляньте декілька прикладів програмного забезпечення Keylogger. 3. Укажіть яким чином Keylogger можуть використовувати зловмисники. *Література:* *https://cryptoacademy.com.ua/shho-take-kejlogger/*	2
4	*ПР № 4. Генерування і використання електронного цифрового підпису для реалізації захисту файлів користувача.* План: 1. Створити власний електронний підпис для документів, створених в додатках MS Office 2. Написати есе «Електронний цифровий підпис» 3. Підписати файл *Література: Гапак О. М. с.146-151*	2
	Тема 1.4 Безпека Інтернет-застосувань	

№	Назва теми	Кількість годин
5	*ПР №5. Робота з криптографічними засобами шифрування інформації.* План: 1. Встановлення та налаштування програмного засобу криптографічного захисту інформації на інформаційних носіях "Crypto Expert". 2. Зашифрувати інформацію за допомогою криптографічного захисту інформації на інформаційних носіях "Crypto Expert". 3. Налаштування брандмауерів та мережевих екранів. *Література: Гапак О. М. с.169*	2
	Всього годин	**10**

6 ТЕМИ І ПИТАННЯ ДО САМОСТІЙНОЇ РОБОТИ СТУДЕНТА

Тема. Концепція захисту інформації та інформаційних технологій. Категорії комп'ютерної безпеки. (5 годин)

План:

1. Захист компонентів ОС.
2. Захист баз даних.
3. Налаштування системи захисту СУБД.
4. Цілісність баз даних, системи резервного копіювання.
5. Проблема спільного доступу.
6. Керування доступом до ресурсів ОС.
7. Механізми сучасних апаратних платформ, що використовуються для підтримки функціонування підсистеми захисту ОС.

Література: Гапак О. М. с. 5-7

Форма контролю: опитування.

Тема. Правове регулювання обігу та захисту інформації. (5 годин)

План:

1. Треті особи, одержувач та Уповноважений ВРУ з прав людини.
2. Законність обробки персональних даних.

3. Достовірність та точність даних що обробляються.
4. Підстави обробки персональних даних.
5. Права суб'єкта персональних даних.

Література: Бем М. В., с. 19-70

Форма контролю: опитування.

Тема. Основні види загроз конфіденційності інформації. (5 годин)

План:

1. Технічні можливості зловмисника і засоби знімання інформації.
2. Технічні засоби захисту даних від їх витоку.
3. Основні напрями комп'ютерних злочинів.
4. Базові схеми атак
5. Організація каналів витоку інформації

Література: Гапак О. М. с. 14-21

Форма контролю: опитування

.

Тема. Основні методи захисту ПЗ: від вірусів, від незадекларованих можливостей ПЗ. (5 годин)

План:

1. Політика безпеки.
2. Побудова системи захисту.
3. Основні підсистеми комплексу засобів захисту.

Література: Гапак О. М. с. 21-27

Форма контролю: опитування.

Тема. Організація системи захисту інформації. Політика безпеки. (5 годин)

План:

1. Критерії оцінювання захищених комп'ютерних систем.
2. Законодавча і нормативна база захисту інформації в України.
3. Міжнародний стандарт ISO/IEC 15408.
4. Ідентифікація та аутентифікація.

Література: Гапак О. М. с. 40-61

Форма контролю: опитування.

Тема. Електронний цифровий підпис. (5 годин)

План:

1. Використання ЕЦП в банківській системі.
2. Основні правила безпечного використання ЕЦП.
3. Створення ЕЦП в банківській системі використовуючи їх додатки.

Література: Гапак О. М. с. 146-151

Форма контролю: опитування.

Тема. Захист інформації шляхом перетворення. Криптографічні вимоги до захисту інформації. Особливості стеку мережевих протоколів. (6 годин)

План:

1. Основні види сучасних криптоалгоритмів і шифрів.
2. Універсальні методи криптозахисту
3. Проблеми реалізації методів криптографічного захисту ПК, серверів, мереж.
4. Елементи криптоаналізу.
5. Елементарна криптографія.

Література: Гапак О. М. с. 169-174

Форма контролю: опитування.

7 МЕТОДИ АКТИВІЗАЦІЇ НАВЧАЛЬНОГО ПРОЦЕСУ

Класичні лекції, лекції-бесіди, індивідуальні консультації для студентів, лекції проблемного характеру, розв'язування ситуаційних задач.

СИСТЕМА ПОТОЧНОГО І ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ

Для визначення рівня засвоєння студентами навчального матеріалу використовуються наступні методи оцінювання знань:

1. Поточне оцінювання;
2. Тематичне оцінювання;
3. Оцінки за індивідуальну самостійну роботу;
4. Семестрове оцінювання, залік.

ПИТАННЯ ТА ЗАВДАННЯ ДО ЗАЛІКУ З ДИСЦИПЛІНИ «ЗАХИСТ ІНФОРМАЦІЇ ТА БЕЗПЕКА ПК МЕРЕЖ»

1. Захист компонентів ОС.
2. Захист баз даних.
3. Налаштування системи захисту СУБД.
4. Цілісність баз даних, системи резервного копіювання.
5. Проблема спільного доступу.
6. Керування доступом до ресурсів ОС.
7. Механізми сучасних апаратних платформ, що використовуються для підтримки функціонування підсистеми захисту ОС.
8. Технічні можливості зловмисника і засоби знімання інформації.
9. Технічні засоби захисту даних від їх витоку.
10. Основні види сучасних криптоалгоритмів і шифрів.
11. Проблеми реалізації методів криптографічного захисту ПК, серверів, мереж.
12. Стенографічні методи захисту інформації.
13. Використання особливостей структури файлу (кодування молодшим бутом, підміна високочастотних складових в мультимедійних

додатках).

14. Використання особливостей візуалізації даних.

15. Побудова і аналіз збуджень спектральних характеристик сигналу як можливість наявності секретної інформації. Шифри, коди та їх призначення.

16. Елементи криптоаналізу.

17. Елементарна криптографія.

18. Шифрування блоками.

19. Дешифрування ітераціями.

20. Концепція відкритих систем.

21. Система RSA, її опис, коректність, надійність.

22. Пакет захисту PGP.

23. Генератори псевдовипадкових бітів.

24. Протоколи обміну ключами.

25. Ідентифікація за допомогою симетричної криптосистеми, на основі цифрового підпису.

26. Визначення міжмережних екранів (МЕ).

27. Принципи побудови та класифікації МЕ.

28. Моделі порушника, загроз та обмеження МЕ.

29. Розвиток технології МЕ.

30. Системи моніторингу.

31. МЕ основних світових виробників.

32. Основні типи засобів забезпечення інформаційної безпеки в розподілених обчислювальних середовищ та мережах.

33. Основи систем аналізу вразливостей.

34. Основи систем виявлення вторгнень.

35. Три принципи побудови систем виявлення вторгнень.

36. Особливості забезпечення захисту комп’ютерних систем сполучених з глобальною мережею Інтернет.

37. Вразливості протоколів Інтернет.

38. Особливості загрози типу «відмова в обслуговуванні».

39. Характеристика інструментальних засобів захисту.

40. Політика безпеки при використанні ресурсів мережі Інтернет.

41. Захист електронної пошти від вірусів та спаму.

42. Методи розпізнавання спаму: чорні та білі списки.

43. Використання методів штучного інтелекту для розпізнавання спаму.

44. Механізми та засоби захисту від шкідливих та небезпечних програм.

45. Засоби і прийоми для профілактики і захисту.

46. Антивірусне програмне забезпечення профілактика вірусного зараження.

47. Електронний цифровий підпис.

48. Підстави для обробки персональних даних.

КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Відповідно до ступеня оволодіння зазначеними знаннями і способами діяльності виокремлюються такі рівні навчальних досягнень студентів з даної дисципліни:

Оцінка	Критерії
Незадовільно	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових розрахунків, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності. Безсистемне відділення випадкових ознак вивченого.
Задовільно	В цілому володіє навчальним матеріалом, викладає його основний зміст під час усних виступів та письмових розрахунків, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину практичних завдань.
Добре	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому нормативну та обов’язкову літературу. Правильно вирішив більшість практичних завдань. Студент здатен виділяти суттєві ознаки вивченого за допомогою операцій синтезу, аналізу, виявляти причинно- наслідкові зв’язки, у яких можуть бути окремі несуттєві помилки, формувати висновки і узагальнення, вільно оперувати фактами та відомостями.
Відмінно	В повному обсязі володіє навчальним матеріалом з дисципліни, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей (практичні роботи, контрольні роботи тощо), глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому нормативну, обов’язкову та додаткову літературу з дисципліни. Правильно вирішив усі практичні завдання. Студент здатен виділяти суттєві ознаки вивченого за допомогою операцій синтезу, аналізу, виявляти причинно- наслідкові зв’язки, сформувати висновки і узагальнення.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

ОСНОВНА

1. Бем М. В., Городиський І. М. Стандарти захисту персональних даних в соціальній сфері. нав. посібник, 2018.
2. Гапак О. М. Захист інформації в комп'ютерних системах: нав. посібник. Ужгород, 2021.
3. Гуз А. М., Касперський І. П., Князєв С. О. Організація захисту інформації з обмеженим доступом: нав. посібник. Київ, 2018.

ДОДАТКОВА

4. Гуз А. М., Касперський І. П., Князєв С. О. Охорона державної таємниці в Україні: нав. посібник. Київ, 2017.
5. Касперський І. П., Князєв С. О. Організаційно-правові основи захисту службової інформації: нав. посібник. Київ, 2017.
6. Супруненко А. М., Башта І. І., Лисеюк А. М., Свіріна К. С. Організація охорони державної таємниці в Україні: нав. посібник. Ірпінь, 2020.
7. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія. / Науково-дослідний інститут інформатики і права НАПрН України, 2019.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Про Державну таємницю: Закон України із змінами і доповненнями, внесеними Законом України від 21.09.1999 №1079-XIV. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
2. Про захист інформації в автоматизованих системах: Закон України від 05.07.94 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
3. Про зв'язок: Закон України із змінами, внесеними згідно із Законом від 04.07.2002 № 36-IV-ВР. URL: https://zakon.rada.gov.ua/laws/show/160/95-вр#Text

4. Про інформацію: Закон України із змінами, внесеними згідно із Законом від 07.02.2002 № 3047-III-ВР. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
5. Про науково-технічну інформацію: Закон України від 25.06.93 № 3323-XII-ВР. URL: https://zakon.rada.gov.ua/laws/show/3322-12#Text
6. Про Національну програму інформатизації: Закон України із змінами, внесеними згідно із Законом від 13.09.2001 № 2684-III-ВР. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text
7. Про основи національної безпеки України: Закон України від 15 грудня 2005 року № 3200-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text

ДОДАТКИ

Зразок питань для усного опитування.

1. Який вигляд має шифр Цезаря?
2. Дайте визначення терміну Електронно цифровий підпис.
3. Які існують загрози втрати інформації в ПК?
4. Яким чином зловмисник може отримати доступ до приватної інформації.
5. Назвіть види шифрування.

Зразок тестових завдань

1. Яку назву має приєднане до тексту криптографічне перетворення, що дозволяє при одержанні тексту іншим користувачем перевірити авторство і дійсність повідомлення?

а) система автоматизації;

б) система документообігу;

в) електронний (цифровий) підпис;

г) ключ;

д) САДД.

2. Вид ідентифікації, який ґрунтується на визначенні особистості користувача за певним предметом, ключем, що перебуває в його ексклюзивному користуванні.

а) апаратна ідентифікація;

б) аутентифікація;

в) парольна ідентифікація;

г) біометрична ідентифікація;

д) алгоритмічна ідентифікація.

3. Програми, що на перший погляд є стовідсотковими вірусами, але не спроможні розмножуватися через помилки.

а) кодувальники;

б) конструктори вірусів;

в) поліморфік-генератори;

г) троянські коні;

д) intended-віруси.

4. Процес перетворення звичайної інформації (відкритого тексту) в шифротекст.

а) дешифрування;

б) шифрування;

в) стійкість;

г) аналіз;

д) кодування.

5. Секретний параметр (в ідеалі, відомий лише двом сторонам) для окремого контексту під час передачі повідомлення?

а) дешифрування;

б) шифрування;

в) ключ;

г) криптостійкість;

д) кодування.

Приклад різнорівневого завдання.

Початковий рівень – 0,5 бала

1. **Ідентифікація людини за унікальними, властивими тільки їй ознаками.**

а) апаратна ідентифікація;

б) аутентифікація;

в) парольна ідентифікація;

г) біометрична ідентифікація;

д) алгоритмічна ідентифікація.

2. Кожен зареєстрований користувач системи одержує набір персональних реквізитів. Далі при кожній спробі входу людина повинна вказати свою персональну інформацію, що називається…

а) апаратна ідентифікація;

б) аутентифікація;

в) парольна ідентифікація;

г) біометрична ідентифікація;

д) алгоритмічна ідентифікація.

3. Які програми постійно зберігаються у пам’яті комп’ютера й у визначений користувачем час перевіряють оперативну пам’ять комп’ютера, файли, BOOT-сектор, FAT-таблицю?

а) детектори;

б) фаги;

в) вакцини;

г) сторожі;

д) ревізори.

4. Загрози поділяються на:

а) системні та адміністративні;

б) природні та штучні;

в) глобальні та локальні;

г) однорівневі та багаторівневі;

д) індукційні та електромагнітні.

Середній рівень – по 0,5 балів

1. **Укажіть відповідність між поняттями і визначеннями.**

1. Детектори	А) Антивірусні програми використовуються для обробки файлів і boot-секторів із метою попередження зараження відомими вірусами
2. Фаги	Б) Антивірусні програми призначені для знаходження заражених файлів одним із відомих вірусів.
3. Вакцини	В) резидентні програми, які постійно зберігаються у пам'яті комп'ютера й у визначений користувачем час перевіряють

	оперативну пам'ять комп'ютера, файли, BOOT-сектор, FAT-таблицю.
4. Сторожі	Г) виявляють та знешкоджують вірус (фаг) або кілька вірусів.

2. **Укажіть відповідність між поняттями і визначеннями.**

1. Конструктори вірусів	А) це шкідлива програма, яка вміло проникає в систему під виглядом легального додатку або програмного забезпечення.
2. Троянські коні	Б) програми, які, на перший погляд, є стовідсотковими вірусами, але не здатні розмножуватися через помилки.
3. Intended-віруси	В) один з модулів у складі комп'ютерної програми, найчастіше комп'ютерного вірусу, головною функцією котрого є шифрування та дешифрування(зміні) тіла усієї програми або її частини.
4. Поліморфік-генератори	Г) комп'ютерна програма, яка має здатність до прихованого самопоширення.

Достатній рівень – 2 бала

Написати есе на тему “Використання ЕЦП у банківській системі”

Питання для самоконтролю

1. Загальні поняття та положення із захисту інформації

1.1. Складові інформаційної безпеки.

1.2. Дайте визначення поняттю “вірус”.

1.3. Правове регулювання захисту інформації в Україні.

1.4. Які існують основні загрози конфіденційності інформації?

1.5. Яким чином працює “троянський кінь”?

2. Комплексна система захисту інформації

2.1. Яким чином створюється електронно цифровий підпис?

2.2. Дайте визначення терміну “кейлоггер”.

2.3. Криптографічні засоби шифрування інформації.

2.4. Політика безпеки інформації у провідних компаніях.

2.5. Стек мережевих протоколів.