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
Людмила ПУСТОВОЙТ
«30» серпня 2023 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ВНПП03.04.02 ОСНОВИ КІБЕРБЕЗПЕКИ

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 Основи кібербезпеки для підготовки фахових молодших бакалаврів для IV курсу за освітньо-професійною програмою Обслуговування комп'ютерних систем і мереж спеціальності 123 Комп'ютерна інженерія.

РОЗРОБНИКИ ПРОГРАМИ: Олена Ленченко – викладач вищої категорії, старший викладач

Робочу програму схвалено на засіданні циклової комісії комп'ютерно-інтегрованих технологій

Протокол №1 від «27» серпня 2023р.

Голова циклової комісії_____Людмила ГЛУШКО

Розглянуто і рекомендовано до затвердження навчально-методичною радою коледжу

Протокол № 1 від «30» серпня 2023р.

Голова НМР_____Аліна ОДИНЕЦЬ

ЗМІСТ

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 «Основи кібербезпеки» полягає в наданні студентам ключових знань та навичок для розуміння, виявлення та захисту від кіберзагроз. Підготовка студентів до роботи та діяльності в галузі інформаційної безпеки, забезпечення їх здатності ефективно виявляти, уникати та реагувати на кіберзагрози в різних областях, включаючи бізнес, науку та громадянське суспільство.

Завдання дисципліни «Основи кібербезпеки» включає в себе:

- Ознайомлення студентів з основними поняттями, термінологією та принципами кібербезпеки;
- Вивчення конкретних кіберзагроз, які можуть виникнути, і оцінка ризиків, пов'язаних із цими загрозами;
- Тренування студентів у виявленні потенційних кіберзагроз та аналізі їх характеристик;
- Вивчення та розробка стратегій та методів захисту інформації та інфраструктури від кібератак;
- Ознайомлення з сучасними інструментами та технологіями, які використовуються в галузі кібербезпеки;
- Розуміння та протидія методам соціальної інженерії.

Процес вивчення дисципліни ВНПП03.04.02 Основи кібербезпеки спрямований на формування елементів наступних компетентностей:

Загальні компетентності:

КЗ 3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ 4. Здатність спілкуватися державною мовою як усно, так і письмово.

КЗ 7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел та практичного її застосування.

КЗ 8. Здатність вчитися і бути сучасно навченим.

Спеціальні (фахові) компетентності:

КФ 1. 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.

КФ 2. 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.

КФ 8. Здатність використовувати знання сучасних технологій та інструментальних засобів розробки складних програмних систем (інженерії програмного забезпечення), уміння їх застосовувати на всіх етапах життєвого циклу розробки.

КФ 9. Здатність брати участь в модернізації та реконструкції апаратних та програмних засобів комп'ютерної інженерії, зокрема з метою підвищення їх ефективності.

КФ 10. Здатність здійснювати вибір, розробляти, розгортати, інтегрувати, діагностувати, адмініструвати та експлуатувати комп'ютерні системи та мережі, мережеві ресурси, сервіси та інфраструктуру організації.

КФ 11. Здатність до ділових комунікацій у професійній сфері, знання основ ділового спілкування, навички роботи в команді.

КФ 13. Здатність оцінювати і враховувати економічні, соціальні, технологічні та екологічні чинники, що впливають на сферу професійної діяльності.

КФ 14. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати прийняті рішення.

Програмні результати навчання:

РН 1. 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.

РН 2. 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.

РН 5. 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.

РН 6. 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.

РН 12. Вміти застосовувати базові знання стандартів в області інформаційних технологій при розробці та впровадженні інформаційних систем і технологій

РН 14. Володіти навиками аналізу навчальної і спеціальної літератури, нормативних положень, технічної документації для вирішення проблем, що виникають у професійній діяльності.

РН 24. Знати схемотехнічні основи сучасних комп’ютерів, сучасні систем САПР, правила комп'ютерного оформлення креслень.

РН 27. Вміти застосовувати комп’ютерні засоби при проектуванні та створенні апаратних і програмних складових КСМ

РН 28. Вміти опановувати та розробляти документацію на системи, продукти і сервіси інформаційних технологій, професійно спілкуватись рідною та англійською мовою

РН 36.Вміти застосовувати теоретичні (логічні та арифметичні) основи побудови сучасних комп’ютерів при вирішенні професійних завдань.

РН 41. На основі впровадження сучасних методів проектування, створення та експлуатації вміти забезпечити безаварійний стан функціонування глобальних, локальних, мобільних та інших комп’ютерних мереж.

РН 43. Вміти економічно мислити, орієнтуватися у конкретних виробничих ситуаціях, аналізувати показники виробничої діяльності підприємства.

РН 44. Вміти здійснювати контроль за дотриманням норм охорони праці, техніки безпеки, екологічної та протипожежної безпеки, та умов безпеки життєдіяльності

РН 45. Практично володіти рідною та однією з іноземних мов в обсязі тематики, зумовленої професійними потребами.

РН 46. 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

РН 48. Вдосконалювати професійний та особистісний розвиток протягом усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

НАВЧАЛЬНО-ТЕМАТИЧНИЙ ПЛАН

№	Назва розділу	Кількість годин			
		Всього	Л.	Пр.	С.р.
1.	Основи кібербезпеки	12	4	2	6
2.	Мережева безпека. Тенденції в кібербезпеці	48	6	12	30
Всього		**60**	**10**	**14**	**36**

КАЛЕНДАРНО-ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№	Назва розділу, теми, заняття	Кількість годин		
		Л.	Пр.	С.р.
Розділ І. Основи кібербезпеки		**4**	**2**	**6**
1	Введення в кібербезпеку	2		2
2	Встановлення антивірусного програмного забезпечення		2	
3	Основні принципи кібербезпеки	2		4
4	**Розділ ІІ. Мережева безпека. Тенденції в кібербезпеці**	**6**	**12**	**30**
5	Мережева безпека	2		4
6	Захист від вірусів і шкідливих програм			4
7	Конфігурація брандмауера . Використання інтридер-детектора		2	
8	Соціальна інженерія	2		4
9	Захист інформації в хмарних сервісах			2
10	Симуляція соціально-інженерних атак . Захист хмарних сервісів		2	
11	Кіберзахист корпоративних мереж			4
12	Аутентифікація та авторизація користувачів		2	
13	Криптографія у кібербезпеці	2		4

№	Назва розділу, теми, заняття	Кількість годин		
		Л.	Пр.	С.р.
14	Вивчення перших методів шифрування інформації. Шифрування файлів		2	
15	Захист від DDoS-атак. Аналіз журналів подій		2	4
16	Тенденції у кібербезпеці			4
17	Створення плану інцидентного реагування . Проект з застосуванням набутих знань		2	
Всього		10	14	36

ТЕМИ І ПЛАНИ ЛЕКЦІЙНИХ ЗАНЯТЬ

№	Назва теми	К-ть годин
Розділ І. Основи кібербезпеки		
Л-1	Введення в кібербезпеку План: 1. Визначення кібербезпеки та її важливість. 2. Огляд основних загроз і викликів у кіберпросторі. 3. Роль людини у забезпеченні кібербезпеки.	2
Л-2	Основні принципи кібербезпеки План: 1. Принципи конфіденційності, цілісності та доступності. 2. Заходи безпеки: шифрування, аутентифікація, авторизація.	2
Розділ ІІ. Мережева безпека. Тенденції в кібербезпеці		
Л-3	Мережева безпека План: 1. Загрози мережевої безпеки. 2. Засоби захисту мережі: брандмауери, інтридер-детекція, віртуальні приватні мережі (VPN).	2
Л-4	Соціальна інженерія План: 1. Визначення соціальної інженерії.	2

№	Назва теми	К-ть годин
	2. Захист від соціально-інженерних атак.	
Л-5	Криптографія у кібербезпеці План: 1. Основні принципи криптографії. 2. Використання криптографії для захисту інформації.	2
Всього:		**10**

ТЕМИ І ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ

№	Назва теми	К-ть годин
1	Встановлення антивірусного програмного забезпечення План: 1. Крок за кроком налаштування та використання антивірусу.	2
2	Конфігурація брандмауера . Використання інтридер-детектора План: 1. Налаштування брандмауера для захисту мережі. 2. Встановлення та налаштування системи інтридер-детекції.	2
3	Симуляція соціально-інженерних атак . Захист хмарних сервісів План: 1. Проведення вправ імітації соціально-інженерних атак для тренування обізнаності персоналу. 2. Налаштування додаткових заходів безпеки для користування хмарними сервісами.	2
4	Аутентифікація та авторизація користувачів План: 1. Налаштування механізмів аутентифікації та авторизації.	2
5	Вивчення перших методів шифрування інформації. Шифрування файлів План: 1. Зашифрувати інформацію за допомогою шифра Цезаря. 2. Зашифрувати інформацію за допомогою шифру з використання кодового слова.	2

№	Назва теми	К-ть годин
	3. Зашифрувати інформацію за допомогою шифру з простої заміни. 4. Застосування різних методів шифрування для захисту конфіденційної інформації.	
6	Захист від DDoS-атак. Аналіз журналів подій План: 1. Використання спеціальних інструментів для виявлення і захисту від DDoS-атак. 2. Використання інструментів аналізу журналів подій для виявлення можливих загроз.	2
7	Створення плану інцидентного реагування. Проект з застосуванням набутих знань План: 1. Розробка плану дій під час кіберінциденту для ефективного реагування. 2. Розробка та реалізація проекту з області кібербезпеки, включаючи аналіз ризиків, виправлення потенційних вразливостей та рекомендації щодо покращення безпеки.	2
Всього		**14**

ТЕМИ І ПИТАННЯ ДО САМОСТІЙНОЇ РОБОТИ СТУДЕНТА

№	Теми для самостійної роботи	К-ть годин
1	Введення в кібербезпеку План: 1. Що таке кібербезпека і чому вона є важливою сферою в сучасному світі? 2. Які основні загрози і виклики існують у кіберпросторі? 3. Яку роль відіграє людина у забезпеченні кібербезпеки?	2
2	Основні принципи кібербезпеки План: 1. Що включає в себе принцип конфіденційності в контексті кібербезпеки? 2. Чому цілісність є важливим аспектом в системах	4

№	Теми для самостійної роботи	К-ть годин
	інформаційної безпеки? 3. Яким чином можна забезпечити доступність інформації в умовах кіберзагроз? 4. Що означає аутентифікація та чому це важливо для безпеки систем? 5. Які переваги вносить авторизація в процес забезпечення кібербезпеки? 6. Які можливі ризики можуть виникнути, якщо принципи конфіденційності, цілісності та доступності порушуються? 7. Що таке шифрування і як воно допомагає забезпечити конфіденційність інформації? 8. Які основні етапи включає процес аутентифікації користувача?	
3	Мережева безпека План: 1. Які загрози і виклики стикаються мережеві системи? 2. Які принципи можна використовувати для захисту мережі від несанкціонованого доступу? 3. Як функціонують брандмауери та як вони допомагають в забезпеченні мережевої безпеки? 4. Які переваги та недоліки використання віртуальних приватних мереж (VPN)? 5. Які основні методи можна використовувати для виявлення та запобігання інтридер-атак? 6. Як забезпечити безпеку мережевої комунікації в публічних бездротових мережах? 7. Які рекомендації ви надаєте для захисту мережевої інфраструктури в корпоративному середовищі? 8. Які механізми можна використовувати для шифрування мережевого трафіку?	4
4	Захист від вірусів і шкідливих програм План: 1. Які є основні типи вірусів та шкідливих програм, які можуть вразити комп'ютерну систему? 2. Як віруси розповсюджуються та яким чином вони можуть потрапити на комп'ютер? 3. Як працюють антивірусні програми і як вони визначають та	4

№	Теми для самостійної роботи	К-ть годин
	нейтралізують загрози? 4. Які основні заходи можна прийняти для захисту від вірусів при використанні електронної пошти? 5. Як можна виявити наявність шкідливого програмного забезпечення на комп'ютері та провести його вилучення? 6. Які стратегії можна використовувати для захисту мобільних пристроїв від вірусів і шкідливих програм? 7. Як використання оновлень програмного забезпечення може сприяти захисту від вірусів? 8. Яким чином можна створити безпечне середовище для завантаження та встановлення програм? 9. Як виявити та уникнути фішингових атак, пов'язаних із поширенням вірусів? 10. Які кроки слід вжити для відновлення інформації, якщо система вже була заражена вірусами?	
5	Соціальна інженерія План: 1. Що таке соціальна інженерія в контексті кібербезпеки і які її основні мети? 2. Які можливі наслідки соціально-інженерних атак для організацій та індивідуальних користувачів? 3. Як використовуються техніки маніпулювання та соціальної інженерії для отримання несанкціонованого доступу до інформації? 4. Як визначити підозрілу соціально-інженерну атаку і яким чином уникнути потенційних загроз? 5. Які стратегії можна використовувати для навчання персоналу впізнаванню та уникненню соціально-інженерних атак? 6. Як впливають соціальні мережі на ризик соціально-інженерних атак? 7. Як можна підвищити свідомість про соціальну інженерію серед користувачів в організаціях?	4
6	Захист інформації в хмарних сервісах План: 1. Які переваги та ризики пов'язані з використанням хмарних сервісів для зберігання та обробки інформації?	2

№	Теми для самостійної роботи	К-ть годин
	2. Як можна забезпечити конфіденційність інформації, зберігаючи її в хмарних сервісах? 3. Які аспекти безпеки слід враховувати при виборі хмарного провайдера? 4. Які механізми шифрування можна використовувати для захисту даних у хмарних сервісах?	
7	Кіберзахист корпоративних мереж План: 1. Які загрози можуть виникати в корпоративних мережах інформаційної безпеки? 2. Які можливі наслідки порушення кіберзахисту корпоративної мережі для бізнесу? 3. Які основні елементи системи інформаційної безпеки корпоративної мережі? 4. Як вивчити та управляти доступом користувачів в корпоративній мережі? 5. Як виявляти та реагувати на потенційні загрози безпеки в корпоративній мережі? 6. Як можна підвищити освідомленість персоналу з питань кібербезпеки в корпоративному середовищі? 7. Яким чином можна захистити конфіденційні дані, що передаються по корпоративній мережі?	4
8	Криптографія у кібербезпеці План: 1. Які основні принципи криптографії використовуються в кібербезпеці? 2. Як шифрування сприяє забезпеченню конфіденційності даних? 3. Які основні методи аутентифікації використовуються в криптографії для перевірки ідентичності сторін? 4. Яким чином цифровий підпис забезпечує цілісність даних та аутентифікацію відправника? 5. Як використовуються хеш-функції в криптографії для забезпечення цілісності інформації? 6. Які переваги та недоліки симетричного та асиметричного шифрування?	4

№	Теми для самостійної роботи	К-ть годин
	7. Як криптографія використовується для захисту паролів та інших конфіденційних даних?	
9	Захист від DDoS-атак План: 1. Що таке DDoS-атака і які її основні характеристики? 2. Які можливі наслідки DDoS-атак для бізнесу та інтернет-ресурсів? 3. Як відбувається розпізнавання та аналіз DDoS-атак для їх вчасного виявлення? 4. Які види DDoS-атак існують і як вони відрізняються один від одного? 5. Яким чином можна забезпечити захист від DDoS-атак на різних рівнях, включаючи мережевий та застосунковий рівні? 6. Які техніки обходження захисту від DDoS-атак можуть використовуватися зловмисниками? 7. Як можна використовувати CDN (мережу доставки контенту) для захисту від DDoS-атак? 8. Які служби та інструменти використовуються для моніторингу та виявлення DDoS-атак в реальному часі?	4
10	Тенденції у кібербезпеці План: 1. Які основні сучасні тенденції у сфері кібербезпеки вирізняються? 2. Як технології штучного інтелекту та машинного навчання впливають на кібербезпеку? 3. Які виклики виникають внаслідок зростання кількості підключених до Інтернету пристроїв (IoT)? 4. Як кіберзлочинці адаптуються до нових захисних технологій та як це впливає на заходи кібербезпеки? 5. Які нові методи аутентифікації та авторизації використовуються для зміцнення кібербезпеки? 6. Яким чином технології блокчейну можуть використовуватися для забезпечення безпеки даних? 7. Як розвивається сфера квантової криптографії та які вона має перспективи в кібербезпеці? 8. Як великі дані (Big Data) використовуються для виявлення та	4

№	Теми для самостійної роботи	К-ть годин
	протидії кіберзагрозам? 9. Як регуляторні рамки та законодавчі ініціативи впливають на стратегії кібербезпеки? 10. Які тенденції спостерігаються в області облачних технологій та як вони впливають на кібербезпеку?	
Всього		**36**

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 до заліку з дисципліни «основи кібербезпеки»

1. Що таке кібербезпека та чому вона є важливою в сучасному світі?

2. Які принципи конфіденційності, цілісності та доступності важливі для кібербезпеки?

3. Які загрози і виклики існують у кіберпросторі?

4. Які техніки соціальної інженерії можуть використовуватися для атак на користувачів?

5. Які методи можна використовувати для захисту від вірусів та шкідливих програм?

6. Як функціонують брандмауери та як вони можуть захистити мережу?

7. Які стратегії захисту від DDoS-атак можна використовувати?

8. Які основні принципи криптографії використовуються для захисту інформації?

9. Як хмарні сервіси впливають на безпеку інформації та як їх можна захистити?

10. Які тенденції у кібербезпеці можна визначити на сучасному етапі?

11. Налаштування та тестування антивірусного захисту на комп'ютері.

12. Створення та тестування правил брандмауера для захисту мережі.

13. Аналіз соціально-інженерних атак та розробка заходів протидії.

14. Використання криптографії для зашифрування та розшифрування повідомлень.

15. Симуляція DDoS-атаки на тестовому сервері та аналіз впливу.

16. Оцінка ризиків використання хмарних сервісів та розробка стратегії захисту.

17. Розробка та реалізація плану інцидентного реагування на можливу кібератаку.

18. Використання інструментів для виявлення потенційних загроз у мережі.

19. Аналіз нових тенденцій у кібербезпеці та їх вплив на конкретну організацію.

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

Базова (основна)

1. Богуш В.М., Довидьков О.А. Теоретичні основи захищених

інформаційних технологій - К.: ДУІКТ, 2010. - 508 с

2. Богуш В.М., Довидьков О.А. Проектування захищених комп'ютерних систем та мереж, навчальний посібник, -К.; ДУІКТ, 2008. – 500 с.

3. Бурячок В.Л., Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки, підручник, - К.; ПВП «Задруга», 2014. - 222 с

4. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)

5. Навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик. Львів : Видавництво Львівської політехніки, 2019. 580 с.

6. Cyber-Physical Security : Monograph / edit. Clark. – Springer International Publishing, 2017. – ISBN 978-3-319-32822-5 (print) ; 978-3-319-32824-9 (online). 299 p.

7. Enterprise Security : Monograph / edit. Chang. – Springer International Publishing, 2017. – ISBN 978-3-319-54379-6 (print) ; 978-3-319-54380-2 (online). 277 p.

8. Cyber Security. Simply. Make it Happen. : Monograph / edit. Abolhassan. – Springer International Publishing, 2017. – ISBN 978- 3-319-46528-9 (print) ; 978-3-319-46529-6 (online). 127 p.

Додаткова

9. Лабораторний практикум з навчальної дисципліни "Інформаційна безпека". Навчально- практичний посібник / С. В. Кавун, В. В. Носов, В. В. Огурцов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 256 с. (Укр. мов.)

10. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: Наук.-практ. посіб./ За заг. ред. Проф. Я.Ю. Кондратьєва. – К., 2004.

11. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. – К., 2006.

12. Методичні рекомендації для виконання лабораторних робіт з

дисципліни АДМІНІСТРУВАННЯ ПРОГРАМНИХ СИСТЕМ І КОМПЛЕКСІВ / [Ю. Є. Добришин,

13. І.О.Чернозубкін]; Університет економіки та права «КРОК» – Київ - 2019. – 49 с.

14. Організація комп'ютерних мереж [Електронний ресурс] : підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Електронні текстові дані (1 файл: 45,7 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.

15. Білоус Л. Ф. Інформаційні мережі : навч. посібник / Білоус Л. Ф. – К. : Логос, 2015. – 140 с.

16. Контроль та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології : навчальний посібник / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. – Х. : "Компанія СМІТ", 2004. – 544 с

17. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22 https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf

18. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12. 2007 р. № 232. https://tzi.com.ua/downloads/3.1- 001-07.pdf

Інформаційні ресурси

19. https://www.netacad.com/

20. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

21. https://zakon.rada.gov.ua/laws/show/2297-17#Text

22. https://zakon.rada.gov.ua/laws/show/3855-12#Text

23. https://zakon.rada.gov.ua/laws/show/2657-12#Text

ДОДАТКИ

Зразок питань для усного опитування.

1. Які основні принципи кібербезпеки, які вам вдалося вивчити, ви вважаєте найбільш важливими для захисту інформації?
2. Як ви пояснили б комбінацію конфіденційності, цілісності та доступності в контексті кібербезпеки?
3. Які основні загрози мережевої безпеки ви визнаєте найбільш серйозними, і як їх можна запобігти чи пом'якшити?
4. Які стратегії ви рекомендуєте для захисту від соціально-інженерних атак, особливо в організаційному середовищі?
5. Як ви оцінюєте важливість використання криптографії в кібербезпеці, і які методи ви вважаєте найбільш ефективними для захисту інформації?

Зразок тестових завдань

1. *Яким чином можна описати принцип конфіденційності в контексті кібербезпеки?*

a) Забезпечення доступності інформації

b) Забезпечення цілісності інформації

c) Забезпечення конфіденційності інформації

d) Забезпечення доступу до інформації

2. *Яка техніка захисту від вірусів використовується для виявлення та блокування вірусів на основі їх характеристик?*

a) Фільтрація вмісту

b) Пошук відповідних сигнатур

c) Шифрування файлів

d) Віртуалізація

3. *Що означає аутентифікація в контексті кібербезпеки?*

a) Забезпечення конфіденційності інформації

b) Підтвердження ідентичності користувача

c) Забезпечення доступності інформації

d) Виявлення вірусів у системі

4. Якій техніці захисту від DDoS-атак притаманне розподілене витікання трафіку через глобальну мережу комп'ютерів?

a) Шифрування

b) Вірутальні приватні мережі (VPN)

c) Хмарні сервіси

d) Очищення трафіку через сервіси CDN

5. Яке завдання вирішується за допомогою криптографії в контексті кібербезпеки?

a) Захист від DDoS-атак

b) Забезпечення конфіденційності даних

c) Захист від соціально-інженерних атак

d) Автоматизація інцидентного реагування

Приклад різнорівневого завдання.

Завдання: Рівень "Середній" (2 бали)

Опишіть три основні принципи кібербезпеки та наведіть приклади ситуацій, коли ці принципи можуть бути порушені. Дайте рекомендації щодо заходів забезпечення цих принципів в реальних сценаріях, таких як використання електронної пошти та робота з мобільними пристроями.

Завдання: Рівень "Високий" (3 бали)

Розгляньте сучасні тенденції у кібербезпеці, такі як роль штучного інтелекту та машинного навчання. Поясніть, як ці технології можуть використовуватися для виявлення та протидії кіберзагрозам. Наведіть приклади впровадження таких рішень в реальних організаціях та оцініть їхню ефективність.

Завдання: Рівень "Експерт"

Розробіть план заходів кібербезпеки для великої міжнародної корпорації, яка використовує хмарні сервіси для зберігання та обробки конфіденційної інформації клієнтів. Зазначте ключові елементи стратегії, такі як захист від внутрішніх та зовнішніх загроз, управління доступом, шифрування, та

моніторинг. Поясніть, як ваш план враховує сучасні виклики у сфері кібербезпеки та технологічні тенденції.

Питання для самоконтролю

Розділ І. Основи кібербезпеки

1.1. Що означає термін "кібербезпека" і чому вона є важливою в сучасному інформаційному суспільстві?

1.2. Які основні принципи кібербезпеки і як вони взаємодіють між собою для забезпечення цілісності, конфіденційності та доступності інформації?

1.3. Які загрози і виклики існують у кіберпросторі, і як організації можуть їм протистояти?

1.4. Яким чином соціальна інженерія може бути використана для атак на інформаційну безпеку та як уникнути її негативних наслідків?

1.5. Які стратегії можна використовувати для захисту від вірусів та інших шкідливих програм, що загрожують інформаційній безпеці?

Розділ ІІ. Мережева безпека. Тенденції в кібербезпеці

2.1. Які основні тенденції в мережевій безпеці спостерігаються на сучасному етапі розвитку інформаційних технологій?

2.2. Як вирізняються загрози мережевої безпеки в області хмарних технологій порівняно з традиційними локальними мережами?

2.3. Як технології штучного інтелекту використовуються для виявлення та протидії мережевим загрозам?

2.4. Які заходи безпеки рекомендується вживати для захисту великих мереж в умовах зростання обсягів та складності трафіку?

2.5. Як криптографія взаємодіє з мережевою безпекою, зокрема при передачі даних через великі відстані?

2.6. Як використання мобільних пристроїв та розподілених робочих мереж впливає на стратегії мережевої безпеки?

2.7. Які тенденції у сфері виявлення та реагування на інциденти впливають на вдосконалення мережевої безпеки?

2.8. Як блокчейн може забезпечити покращену безпеку мереж та транзакцій, особливо в контексті криптовалют?

2.9. Як розгортання Інтернету речей (IoT) змінює вимоги до мережевої безпеки та як цим викликам можна відповісти?

2.10. Як законодавчі зміни та регуляції впливають на стратегії та підходи до мережевої безпеки?