Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського
Спеціальна кафедра № 5

ОСНОВИ СТВОРЕННЯ КСЗІ ТА АУДИТ КІБЕРБЕЗПЕКИ

Робоча програма навчальної дисципліни (силабус)

Рівень вищої освіти	*Перший (бакалаврський)*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки*
Освітньо-професійна програма	*Комп'ютерні системи і технології спеціального зв'язку*
Статус дисципліни	*Нормативна*
Форма навчання	*Очна (Денна)*
Рік підготовки, семестр	*IV рік підготовки, осінній семестр*
Обсяг дисципліни	*3 кредити*
Семестровий контроль / контрольні заходи	*Залік*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лекції: Ігор ЯКОВІВ* *Практичні / Семінарські: Ігор ЯКОВІВ*
Розміщення курсу	*Google Classroom*

Київ – 2022

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Силабус освітнього компонента "Основи створення КСЗІ та аудит кібербезпеки" складено відповідно до освітньої програми підготовки бакалаврів "Комп'ютерні системи і технології спеціального зв'язку" спеціальності 122 – Комп'ютерні науки.

Метою навчальної дисципліни є формування та закріплення у курсантів наступних компетентностей: (ЗК1) Здатність до абстрактного мислення, аналізу та синтезу; (ЗК2) Здатність застосовувати знання у практичних ситуаціях; (ЗК3) Знання та розуміння предметної області та розуміння професійної діяльності; (ЗК6) Здатність вчитися й оволодівати сучасними знаннями; (ЗК8) Здатність генерувати нові ідеї (креативність); (ЗК11) Здатність приймати обґрунтовані рішення; (СК3) Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв'язності та нерозв'язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем; (СК12) Здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення; (СК14) Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури; (СК18) Здатність до проектування архітектури інформаційно-комунікаційних систем державних інформаційних ресурсів (ІКС ДІР), вибору і інтегруванню сертифікованих компонентів технічного і стандартного програмного забезпечення при реалізації технології обробки інформації з обмеженим доступом (ІзОД); (СК19) Здатність забезпечувати інформаційну безпеку ІКС ДІР (в тому числі і ІКС для обробки ІзОД), формувати вимоги до комплексних систем захисту інформації (КСЗІ) з підтвердженою відповідністю, забезпечувати проведення їх державної експертизи і ефективну експлуатацію, забезпечувати виконання вимог державної політики кіберзахисту.

Предмет навчальної дисципліни – сутність кіберпростору, концептуальна модель кібербезпеки, державне регулювання кіберзахисту інформації в інформаційно-комунікаційних системах (ІКС), державні інформаційні ресурси (ДІР), інформація з обмеженим доступом (ІзОД), комплексна система захисту інформації (КСЗІ), умови обробки та забезпечення захисту інформації, структура КСЗІ і порядок її створення, кіберзахист об'єктів критичної інфраструктури.

Програмні результати навчання, на формування та покращення яких спрямована дисципліна: (ПР1) Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук; (ПР2) Використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв'язання задач теоретичного та прикладного характеру в процесі проектування та реалізації об'єктів інформатизації; (ПР11) Володіти навичками управління життєвим циклом програмного забезпечення, продуктів і сервісів інформаційних технологій відповідно до вимог і обмежень замовника, вміти розробляти проектну документацію (техніко-економічне обґрунтування, технічне завдання, бізнес-план, угоду, договір, контракт); (ПР14) Знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення; (ПР16) Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

2. Пререквізити та постреквізити навчальної дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Для успішного засвоєння дисципліни курсант повинен володіти освітніми компонентами “Теорія прийняття рішень”, “Побудова та функціонування комп’ютерних систем”, “Засоби і комплекси криптографічного захисту інформації”. Компетенції, знання та уміння, одержані в процесі вивчення освітнього компонента є необхідними для подальшого вивчення освітніх компонентів “Проектування інформаційних систем”, “Переддипломна практика (Військове стажування)”, “Дипломне проектування”.

3. Зміст навчальної дисципліни

Семестр 7

Семестровий (кредитний) модуль 1. Основи створення КСЗІ та аудит кібербезпеки.

Тема 1. Захист інформації в інформаційно-комунікаційних системах.

Кіберпростір як фізичне середовище на основі інформаційно-комунікаційних систем (ІКС). Кібербезпека і захист інформації. Безпека інформаційних процесів. Умови обробки та забезпечення захисту інформації в ІКС. КСЗІ із підтвердженою відповідністю і обґрунтування необхідності її створення. Склад типової інформаційної (автоматизованої) системи. Структура ІКС. Організаційні засади та напрямки захисту інформації. Вимоги до забезпечення захисту інформації. Забезпечення режиму секретності під час обробки інформації, що становить державну таємницю.

Тема 2. Концепція захисту і політика безпеки інформації.

Концепція захисту інформації. Загрози інформації. Модель загроз. Політика безпеки інформації і порядок розробки. Правила розмежування доступу до інформаційних ресурсів. Моделі розподілу доступу. Напрями захисту інформації в ІКС.

Тема 3. Захист від несанкціонованих дій з інформацією.

Сутність несанкціонованих дій (НСД) в ІКС, їх класифікація. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. Класифікація інформаційних (автоматизованих) систем і функціональні профілі захищеності від НСД. Порядок визначення стандартних функціональних профілів захищеності та сертифікованих засобів захисту від НСД.

Тема 4. Захист від витоку каналами побічних електромагнітних випромінювань і наведень.

Технічний канал витоку (ТКВ) і його інформаційно-функціональна структура. Технологічний і небезпечний сигнали. Класифікація ТКВ. Об’єкти інформаційної діяльності (ОІД). Об’єкти ЕОТ. Категоріювання ОІД. Організація захисту інформації від витоку каналами ПЕМВН. Обстеження (в тому числі технічний контроль) об’єктів ЕОТ. Основні рекомендації з технічного захисту інформації від витоку каналами ПЕМВН. Порядок визначення сертифікованих засобів технічного захисту. Технічний контроль за ефективністю вжитих заходів.

Тема 5. Основи забезпечення кібербезпеки.

Концепція кібербезпеки (ІТ-безпеки). Вразливості, загрози, атаки. Аналіз середовищ функціонування. Модель загроз, ризики і політика безпеки. Організаційний захист. Захист від несанкціонованих дій. Правила і моделі розподілу доступу. Захист від витоку інформації технічними каналами. Захист від фізичного доступу до компонентів системи. Система оперативного кіберзахисту. Критерії захисту. Менеджмент кібервразливостями.

Тема 6. Аудит кібербезпеки ІТ систем.

Базові терміни і визначення: аудит, оцінювання, об’єктивні і суб’єктивні оцінки. Об’єкти і суб’єкти аудиту. Концепція і модель інформаційних процесів аудиту. Зміст і характеристики етапів аудиту. Визначення критеріїв бізнес процесів в системі. Планування аудиту. Засоби та методи збору, нормування і аналізу інформації. Оцінювання ефективності аудиту. Підходи до підготовки звіту з аудиту. Концепція і модель інформаційних процесів аудиту кібербезпеки. Пасивний та активний аудит кібербезпеки. Платформи проведення аудиту кібербезпеки. Методи та засоби перевірки документації, логів, встановлених правил, конфігурування систем, трафіку, цілісності файлів.

4. Навчальні матеріали та ресурси

Основна література

1. Закон України “Про інформацію”.
2. Закон України “Про доступ до публичной інформації”.
3. Закон України “Про захист інформації в інформаційно-комунікаційних системах”.
4. Закон України “Про основні засади забезпечення кібербезпеки України”.
5. Закон України “Про Державну службу спеціального зв’язку та захисту інформації України”.
6. Правила забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах. Затверджено постановою Кабінету Міністрів України від 29 березня 2006 року № 373.
7. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури. Затверджено постановою Кабінету Міністрів України від 19 червня 2019 року № 518.
8. Стратегія національної безпеки України. Затверджено Указом Президента України від 14 вересня 2020 року № 392/2020.
9. Стратегія кібербезпеки України. Затверджено Указом Президента України від 26 серпня 2021 року № 447/2021.
10. Положення про Національний координаційний центр кібербезпеки. Затверджено Указом Президента України від 07 березня 2016 року № 242/2016.
11. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, комунікаційних та інформаційно-комунікаційних системах. Затверджено Указом Президента України від 07 березня 2016 року № 242/2016.
12. Яковів І.Б. Основи побудови комплексної системи захисту інформації для інформаційно-телекомунікаційної системи. Навчальний посібник. Київ: Вид-во ІСЗЗІ НТУУ “КПІ ім. Ігоря Сікорського”, 2016. 88 с.
13. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
14. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-комунікаційних системах.
15. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28 квітня 1999 року № 22.
16. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28 квітня 1999 року № 22.
17. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04 грудня 2000 року № 53.
18. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28 квітня 1999 року № 22.
19. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28 квітня 1999 року № 22.
20. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 20 грудня 2000 року № 60.
21. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
22. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB–сторінки від несанкціонованого доступу.

23. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі.

24. Порядок підключення до глобальних мереж передачі даних. Затверджено постановою Кабінету Міністрів України від 12 травня 2002 року № 522.

25. Yakoviv I. Cybernetic model of the advanced persistent threat. *Information Technology and Security*. 2018. Vol. 6, Iss. 2, pp. 46–58, 2018.

26. Яковів І.Б. Базова модель інформаційних процесів та поведінки системи кіберзахисту. *Information Technology and Security*. 2019. Vol. 7, Iss. 2 (13), P. 134–142.

27. Яковів І.Б. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека. *Information Technology and Security*. 2017. Vol. 5, Iss. 2. P. 134–144.

28. Програмне та апаратне забезпечення Навчального ситуаційного центру з кібербезпеки: SOC, SIEM Splunk, Kali Linux, IDS/ IPS Fortigate.

29. Спеціальна відео-аналітична система контролю та безпеки Навчального ситуаційного центру з кібербезпеки.

Додаткова література

1. Зелена книга з питань захисту критичної інфраструктури в Україні. Збірник матеріалів міжнародних експертних нарад / упоряд. Д.С. Бірюков, С.І. Кондратов; за заг. ред. О.М. Суходолі. К. : НІСД, 2015. 176 с. URL: http://www.niss.gov.ua/public/File/2015_nauk_an_rozrobku/Green%20Paper%20-%20dopovid.pdf.

2. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. *Стратегічні пріоритети*. 2015. № 4 (37). С. 83–93. URL: http://sp.niss.gov.ua/content/articles/files/10-1457002140.pdf.

Навчальний контент

5. Методика опанування навчальної дисципліни

Навчальна дисципліна відноситься до циклу нормативної професійної підготовки в системі підготовки бакалавр за спеціальністю 122 Комп'ютерні науки. Отримані курсантами при вивченні навчальної дисципліни знання і уміння необхідні для успішного засвоєння всього комплексу навчальних дисциплін професійної підготовки, а також здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформування про кіберзагрози та відповідні методи захисту від них.

Навчальний матеріал дисципліни має за мету поетапне вивчення сутності безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, організації і забезпечення функціонування національної системи кібербезпеки; формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом; кіберзахисту критичної інформаційної інфраструктури, державного контролю у цих сферах; координації діяльності всіх суб'єктів національної системи кібербезпеки. При цьому, має місце нарощування обсягу та складності матеріалу, починаючи від комплексу ключових понять кіберпростору і його захисту, до процесу реалізації організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки, та усунення їх наслідків, інформування про кіберзагрози та відповідні методи захисту від них. Дана методика викладання матеріалу буде сприяти підвищенню якості засвоєння знань по навчальних дисциплінах спеціальної підготовки і підвищенню рівня практичних навичок по організації наукових досліджень. Особливості вивчення матеріалу навчальної дисципліни полягають у наступному:

– винесення на лекції питань, що дають цілісне уявлення про предмет вивчення, а також основи національної політики кібербезпеки, пріоритетні напрями захисту, функції суб'єктів кіберзахисту, принципи кіберзахисту об'єктів критичної інфраструктури;

– метою практичних занять є формування здібностей по плануванню і здійсненню організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформування про кіберзагрози та методи захисту від них;

– кожний курсант отримує індивідуальне завдання, яке виконує самостійно в ході практичних занять і самостійної підготовки, звітує за нього;

– в ході самостійної роботи курсанти виконують завдання щодо закріплення знань, отриманих на заняттях, а також самостійно відпрацьовують питання, що потребують індивідуальної поглибленої проробки.

Навчальною програмою передбачено всього 90 годин, у тому числі лекцій – 18 годин, практичних занять – 42 годин. Із загального часу 30 годин відокремлюється на самостійне вивчення курсантами питань навчальної дисципліни, виконання контрольних завдань і підготовку до заліку.

У ході навчальних занять використовуються наступні методи навчання:

– усне викладання матеріалу;

– обговорення учбового матеріалу;

– практична робота в класі та на ПЕОМ із застосуванням програмно-апаратних засобів Навчального ситуаційного центру з кібербезпеки;

– самостійна робота під керівництвом викладача.

Проблемність практичних занять із застосуванням ПЕОМ та програмно-апаратних засобів Навчального ситуаційного центру з кібербезпеки досягається шляхом постановки завдань, вирішення яких вимагає творчого застосування знань і вмінь, отриманих на інших заняттях.

Вивчення навчальної дисципліни будується по принципу ускладнення матеріалу і потребує високої мотивації до оволодіння знаннями, уміннями та навиками. Така мотивація підкріплюється наявністю у складі навчальної дисципліни завершених модулів і чіткої звітності курсантів по результатам опрацювання модулів. Однією з ефективних форм поглиблення знань курсантів є робота у наукових гуртках, що сприяє підвищенню якості підготовки майбутній фахівців. Організаційно-наукова робота проводиться в гуртках, створених на кафедрі. Знання, отримані при вивченні навчальної дисципліни, сприяють розвитку творчого мислення та заохочуванню курсантів до активної участі у роботі в наукових гуртках.

В навчальній дисципліні передбачається використання технічних засобів навчання типу “мультимедійний проектор” та автоматизованих навчальних курсів, які застосовуються для демонстрації наочних дидактичних матеріалів, оперативного відображення принципів організації наукових досліджень, рисунків та інших графічних матеріалів, що значно заощаджує час викладача. У якості дидактичного матеріалу використовуються плакати (слайди) на паперових та електронних носіях та ін. Номери, назви розділів, тем і питання навчальних занять, посилання на літературу, послідовність проведення занять надаються у структурі кредитного модулю.

Структура кредитного модуля

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу		Кількість годин				
		Всього	у тому числі			
			Лекції	Практичні (семінарські	Лабораторні заняття (комп'ютерний	СР
Л 0/1	Вступна лекція.	**4**	2			**2**
Тема 1	**Захист інформації в інформаційно-комунікаційних системах.**	**16**	**2**	**6**		**8**
Заняття 1/1	Основи захисту інформації в ІКС. 1. Визначення основних термінів.	4	2	-		2

	2. Умови обробки та забезпечення захисту інформації. 3. Обґрунтування необхідності створення комплексної системи захисту інформації. Основна література: [1-4, 12] Додаткова література: [26]					
Заняття 1/2	Визначення структури типової інформаційно-комунікаційної системи. 1. Склад типової інформаційної (автоматизованої) системи. 2. Склад інформаційно-комунікаційної системи. 3. Засоби аналізу. 4. Аналіз середовищ функціонування ІС. Основна література: [1-6, 12] Інф.-мат. забезп. [28] Додаткова література: [26]	8	-	4		4
Заняття 1/3	Визначення вимог щодо забезпечення захисту інформації. 1. Організаційні засади та напрямки захисту інформації. 2. Визначення вимог щодо забезпечення властивостей інформації. 3. Визначення вимог щодо реєстрації дій в ІКС. 4. Визначення вимог щодо розподілу доступу до інформації та її обміну між системами. Основна література: [2-4, 12] Інф.-мат. забезп. [28]. Додаткова література: [26]	4	-	2		2
Тема 2	**Концепція захисту і політика безпеки інформації.**	**16**	**2**	**6**		**8**
Заняття 2/1	Концепція захисту інформації. 1. Суб'єкти та об'єкти захисту ІКС. 2. Основні процеси захисту. 3. Вразливості і загрози ІКС. Основна література: [1-4, 12] Інф.-мат. забезп. [28] Додаткова література: [24-26]	4	2	-		2
Заняття 2/2	Розробка моделі загроз. 1. Визначення переліку загроз і їх класифікація. 2. Визначення моделі порушника. 3. Аналіз ризику загроз. 4. Визначення концепції захисту ІКС. Основна література: [1-4, 12] Інф.-мат. забезп. [28] Додаткова література: [24-26]	8	-	4		4
Заняття 2/3	Розробка політики безпеки. 1. Структура політики безпеки і порядок її розробки. 2. Правила і політики розподілу доступу.	4	-	2		2

	3. Визначення основних положень політики для безпеки типової ІКС. *Контрольна робота 1.* Основна література: [4-10, 12] Інф.-мат. забезп. [28] Додаткова література: [24-25]					
Тема 3	**Захист від несанкціонованих дій з інформацією.**	**15**	**2**	**6**		**7**
Заняття 3/1	Основи захисту від несанкціонованих дій з інформацією. 1. Основні визначення. 2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НСД). 3. Класифікація інформаційних (автоматизованих) систем і функціональні профілі захищеності від НСД. Основна література: [4-10, 12] Додаткова література: [28]	4	2	-		2
Заняття 3/2	Визначення вимог щодо захисту від НСД стандартного функціонального профілю захищеності. 1. Порядок визначення. 2. Визначення основних завдань захисту. 3. Визначення стандартного функціонального профілю захищеності. Основна література: [11, 12] Інф.-мат. забезп. [28] Додаткова література: [24-25]	8	-	4		4
Заняття 3/3	Визначення засобів захисту від НСД. 1. Порядок визначення. 2. Визначення основних завдань захисту. 3. Визначення стандартного функціонального профілю захищеності. Основна література: [10, 12] Інф.-мат. забезп. [28] Додаткова література: [24-25]	3	-	2		1
Тема 4	**Захист від витоку каналами побічних електромагнітних випромінювань і наведень.**	**9**	**2**	**4**		**3**
Заняття 4/1	Організація робіт по забезпеченню технічного захисту інформації від витоку каналами ПЕМВН. 1. Технічні канали витоку і їх класифікація. 2. Фізичні процеси в каналах ПЕМВН. 3. Проведення категоріювання об'єктів. Основна література: [4-10, 12] Інф.-мат. забезп. [28] Додаткова література: [11]	3	2	-		1
Заняття 4/2	Проведення обстеження засобів ЕОТ. 1. Загальні положення. 2. Порядок проведення робіт та зміст етапів.	6	-	4		2

	3. Особливості застосування засобів технічного контролю. 4. Аналіз результатів обстеження та визначення засобів ТЗІ. *Контрольна робота 2.* Основна література: [4-10, 12] Інф.-мат. забезп. [28] Додаткова література: [11]					
Тема 5	**Основи забезпечення кібербезпеки.**	**20**	**4**	**8**		**8**
Заняття 5/1	Інформаційно-комунікаційні системи і концепція кібербезпеки. 1. Кібербезпека і захист інформації. 2. Кіберпростір як фізичне середовище. 3. Інформаційні процеси в ІКС і їх безпека. 4. Сутність кіберпростору і кібербезпеки. Основна література: [4-10, 12] Інф.-мат. забезп. [28] Додаткова література: [26]	3	2	-		1
Заняття 5/2	Розробка формалізованої моделі системи оперативного кіберзахисту (24/7). 1. Вибір базових визначень та процесів. 2. Визначення структури системи оперативного кіберзахисту (СОК-24/7). 3. Застосування системи визначення вторгнень (IDS). IDS Fortigate. 4. Центр операцій кібербезпеки (SOC) та застосування системи менеджменту подіями та інформацією безпеки (SIEM). SIEM Splunk. Основна література: [4, 7, 26] Інф.-мат. забезп. [27] Додаткова література: [9, 10]	8	-	4		4
Заняття 5/3	Кіберзахист корпоративної інформаційної системи та національна система кібербезпеки. 1. Базові нормативні документи. 2. Моделі процесів управління. 3. Базові процеси національної системи кібербезпеки. 4. Координація дій на рівнях національної системи кібербезпеки. Основна література: [4-7, 26] Додаткова література: [29]	3	2	-		1
Заняття 5/4	Застосування засобів оперативного кіберзахисту. 1. Принципи застосування IDS/ IPS Fortigate. 2. Визначення вторгнень за допомогою IDS/IPS Fortigate. 3. Принципи застосування SIEM Splunk. 4. Збір та аналіз інформації безпеки за допомогою SIEM Splunk. 5. Реалізація відповіді на атаку за допомогою IDS/ IPS Fortigate. Основна література: [4, 7, 26]	6	-	4		2

	Інф.-мат. забезп. [27] Додаткова література: [9, 10]					
Тема 6	**Аудит кібербезпеки ІТ-систем.**	**17**	**4**	**10**		**3**
Заняття 6/1	Концепція аудиту і оцінки кібербезпеки ІТ-систем. 1. Базові визначення. 2. Концептуальна модель. 3. Основні методи аудиту. 4. Засоби збору даних ОС Kali Linux. Основна література: [4-7, 26] Інф.-мат. забезп. [27] Додаткова література: [9, 10]	3	2			1
Заняття 6/2	Визначення характеристик сучасної корпоративної ІТ-системи. 1. Базова модель корпоративної ІТ-системи. 2. Попередній збір інформації про комп'ютерну систему засобами ОС Kali Linux. 2. Аналіз структури комп'ютерної системи. 3. Аналіз інформаційного середовища і технології обробки інформації. 4. Аналіз середовища персоналу. 5. Аналіз фізичного середовища. Основна література: [4-7, 26] Інф.-мат. забезп. [27] Додаткова література: [9,10]	4	-	4		-
Заняття 6/3	Аналіз вимог до забезпечення кібербезпеки корпоративної ІТ-системи. 1. Загальні вимоги щодо кіберзахисту від несанкціонованих дій. 2. Аналіз вимог щодо кіберзахисту доступу до Інтернет. 3. Аналіз вимог щодо сервісу електронної пошти. 4. Аналіз вимог щодо використання зовнішніх носіїв інформації. 5. Застосування SOC, SIEM Splunk, IDS/IPS Fortigate для визначення вразливостей КІС. Основна література: [4-7, 26] Інф.-мат. забезп. [27]. Додаткова література: [9, 10]	5	-	4		1
Заняття 6/4	Тестування на проникнення корпоративних інформаційних систем. 1. Сутність і засоби методу тестування на проникнення. 2. Класифікація і сутність визначення вразливостей системи. 3. Порядок проведення тестування. 4. Засоби тестування. Основна література: [4-7, 26] Інф.-мат. забезп. [27]. Додаткова література: [9,10]	3	2			1

Заняття 6/5	Визначення вразливостей корпоративної інформаційної системи. 1. Визначення характеристик системи. 2. Тестування веб-застосунків засобами ОС Kali Linux. 3. Тестування на проникнення засобами ОС Kali Linux. Основна література: [4-7, 26] Інф.-мат. забезп. [27] Додаткова література: [9, 10]	2	-	2		-
Всього за розділ:		**97**	**18**	**40**	**-**	**39**
Залік		**8**	-	2	**-**	6
Всього:		**105**	**18**	**42**	**-**	**45**

6. Самостійна робота курсанта

Головними видами самостійної роботи курсантів є: самостійна підготовка до аудиторних занять та самостійна підготовка до заліку.

Доцільно час самостійної підготовки для поглибленого вивчення та закріплення навчального матеріалу розподілити наступним чином:

№ з/п	Назва теми та перелік основних питань СР (перелік дидактичного забезпечення, посилання на літературу)	Кількість годин СР
	Вступна лекція	2
1	Тема 1. Захист інформації в інформаційно-комунікаційних системах. 1. Визначте особливості створення КСЗІ для інтегрованих ІКС. Розробите структуру інтегрованої ІКС. 2. Компанія (юридична особа) застосовує комп'ютерні технології для обробки своєї конфіденційної інформації. Визначте напрямки захисту інформації, які мають бути в комплексній системі захисту інформації (КСЗІ) для автоматизованої системи (АС) цієї компанії. Основна література: [3, 12].	8
2	Тема 2. Концепція захисту і політика безпеки інформації. Розробити графічну модель співвідношення вразливості і загрози. Яким чином застосування засобів захисту може бути пов'язано з новими загрозами? Основна література: [3, 12, 23].	8
3	Тема 3. Захист від несанкціонованих дій з інформацією. Яким чином кібербезпека корпоративних систем пов'язана із несанкціонованими діями? Як визначити індикатори компрометації для етапу проникнення моделі СКС? Основна література: [4, 7, 26].	7
4	Тема 4. Захист від витоку каналами побічних електромагнітних випромінювань і наведень. Ознайомитися із засобами інструментальної перевірки співвідношення сигнал/шум фірми Rohde&Shwarz. Основна література: [12].	3
5	Тема 5. Основи забезпечення кібербезпеки. Визначте перелік найбільш рейтингових баз кібервразливостей. Визначте їх особливості. Основна література: [7, 12, 26].	8
6	Тема 6. Аудит кібербезпеки ІТ-систем.	3

	Визначте класифікацію дій із тестування корпоративної IT-системи за методикою PTES. Основна література: [7, 12, 26].	
7	Залік	6
	Всього:	**45**

В рамках самостійної роботи курсанти визначають вимоги захисту щодо означеного сервісу інформаційної системи. Завдання виконується поетапно відповідно до вивчених в ході лекційних та практичних занять методів забезпечення кіберзахисту. Звітність по виконанню завдань самостійної роботи курсанта оформлюється в вигляді публічного захисту.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Політика навчальної дисципліни визначає наступну систему вимог:

– відвідування курсантами занять навчальної дисципліни проводиться відповідно до поточного розкладу занять;

– курсант зобов'язаний опрацювати навчальний матеріал всіх занять із якістю, що забезпечує формування професійних здатностей, які зазначені метою навчальної дисципліни;

– поведінка курсанта на заняттях не повинна заважати ефективному засвоєнню навчального матеріалу та виконанню своїх обов'язків всіма учасниками навчального процесу;

– курсант забезпечує своєчасне та якісне виконання всіх навчальних завдань із дотриманням вимог академічної доброчесності.

У випадку запровадження обмежувальних заходів, що унеможливлюють організацію і здійснення освітнього процесу в навчальних приміщеннях у складі груп, проведення навчальних занять з даної начальної дисципліни можна здійснювати віддалено з використанням технологій дистанційного навчання.

Навчальні матеріали та ресурси, зазначені у розділі 4 цієї робочої програми навчальної дисципліни (силабусі) є відкритими, не містять відомостей з обмеженим доступом і можуть бути оприлюднені з використанням технологій дистанційного навчання, а сама програма не потребує коригування у випадку проведення навчальних занять у дистанційному режимі.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

8.1. Види контролю.

Основні види контролю, які застосовуються в процесі вивчення навчальної дисципліни:

– поточне опитування на лекційних та практичних заняттях;

– контрольна робота;

– публічний захист матеріалів курсанта за завданнями самостійної роботи;

– підсумковий контроль.

Поточний контроль рівня і якості знань, навичок та вмінь здійснюється при проведенні всіх видів занять. Він стимулює систематичну роботу курсантів над матеріалом навчальної дисципліни та забезпечує його своєчасне засвоєння і закріплення у кожній темі.

Поточна контрольна робота, як засіб поточного контролю рівня засвоєння навчального матеріалу, проводяться в ході навчання після вивчення блоку пов'язаних між собою тем навчальної дисципліни. Метою цього виду контролю має бути визначення глибини теоретичної підготовки та сформованості практичних навичок з вивчених тем.

Заплановано проведення двох контрольних робіт.

Контрольна робота № 1.

Формування загальних вимог до КСЗІ для ІКС, що оброблює ІзОД.

Робота виконується після вивчення Теми 2 курсу, проводиться в формі виконання контрольних завдань (тривалість – до 30 хвилин). В рамках роботи курсанти мають дати розгорнуті письмові відповіді на 5 з наступних запитань:

1. Яка інформація відноситься до інформації з обмеженим доступом?
2. Яка інформація відноситься до таємної інформації?/
3. Яка інформація про фізичну особу відноситься до персональних даних?
4. Яка інформація повинна оброблятися в інформаційно-комунікаційній системі із застосуванням КСЗІ з підтвердженою відповідністю?
5. Які напрями захисту можуть бути забезпечені в комплексній системі захисту інформації (КСЗІ)?
6. Які напрями захисту мають бути забезпечуватися в комплексній системі захисту інформації (КСЗІ) під час обробки інформації, що віднесена до державної таємниці?
7. Приватна компанія (юридична особа) застосовує комп'ютерні технології для обробки своєї конфіденційної інформації. Визначте напрямки захисту інформації, які мають бути реалізовані в комплексній системі захисту інформації (КСЗІ) для автоматизованої системи (АС) цієї компанії.
8. Міністерство у своїй автоматизованій системі обробляє тільки інформацію з грифом "цілком таємно". Визначте напрямки захисту інформації, які мають бути реалізовані в комплексній системі захисту інформації (КСЗІ) для автоматизованої системи (АС) цього міністерства.
9. Приватна страхова компанія застосовує комп'ютерні технології для обробки інформації про своїх клієнтів. Визначте напрямки захисту інформації, які мають бути реалізовані в комплексній системі захисту інформації (КСЗІ) для автоматизованої системи (АС) цієї компанії.
10. Державне агентство оброблює службову інформацію в АС на основі локальної мережі. Чи може бути організований обмін даними через Інтернет між комп'ютером цієї мережі і комп'ютером філії агентства?
11. Дайте визначення термінам *вразливість ІКС, загроза інформації ІКС, атака на інформацію ІКС*.
12. Які заходи реалізуються в рамках КСЗІ?
13. Назвіть етапи життєвого циклу ІКС, на яких реалізуються заході захисту інформації.
14. Що таке дані? Що являється носіями інформації в ІКС? Що таке *інформаційній потік* в ІКС?
15. Як можливо класифікувати загрози в ІКС?
16. Дайте визначення політиці безпеки інформації в ІКС. Основні компоненти її структури.
17. Як політика безпеки інформації в ІКС співвідноситься із правилами розподілу доступу (ПРД)?
18. Які основні компоненти політики безпеки інформації в ІКС?
19. Що таке ПРД? Основні формалізовані моделі розмежування доступу.
20. Дайте визначення термінам *інформаційний об'єкт, інформаційний суб'єкт, інформаційний процес.*
21. Яку модель політики доступу можливо описати за допомогою матриці доступу (access matrix)?
22. Сутність *мандатного управління доступом* (МП, Mandatory Access Control – MAC).
23. Сутність *рольової політики розподілу доступу* (РП, Role Base Access Control – RBAC).
24. Які напрямки захисту можуть бути реалізовані в рамках КСЗІ?
25. Який нормативний документ визначає порядок створення КСЗІ для ІКС, в яких обробляється інформація, яка є власністю держави, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством?

26. Перелічите основні компоненти КСЗІ для ІКС, в яких обробляється інформація, яка належить до державної таємниці.

Контрольна робота № 2**.**

Принципи та засоби захисту від НСД та технічних каналів витоку.

Робота виконується після вивчення теми 4 дисципліни, проводиться в формі контрольної роботи тривалістю 30 хвилин. В рамках роботи курсанти мають дати розгорнуті письмові відповіді на 5 з наступних запитань:

1. Дайте визначення термінам *сигнал, технологічний сигнал, небезпечний сигнал*.
2. Дайте визначення терміну *технічний канал витоку інформації (ТКВІ).*
3. Яким чином класифікуються ТКВІ?
4. Які фізичні процеси лежать в основі каналів витоку за рахунок ПЕМВН?
5. Який параметр дозволяє оцінити ступінь небезпеки витоку інформації за рахунок ПЕМВН?
6. Приведіть приклад об’єкту ЕОТ, що містить ДТЗС, які формують технічні канали витоку побічними наводками.
7. Приведіть приклад об’єкту ЕОТ, що містить ДТЗС, які формують технічні канали витоку колами електроживлення.
8. Планується організувати обробку даних з грифом “цілком таємно” на персональному комп'ютері, навколо якого забезпечується контрольована територія з радіусом 15 метрів. В рамках проведення інструментального контролю в трьох напрямах було виявлено небезпечні сигнали побічних електромагнітних випромінювань і наведень (ПЕМВН). Результати вимірювань відносини “небезпечний сигнал / шум” представлені в табл. 1.

Таблиця 1

№ напрямку	Значення відношення “небезпечний сигнал/шум”
1	1,8
2	1,2
3	1,5

У табл. 2 представлений фрагмент норм ефективності захисту інформації в автоматизованих системах від ПЕМВН.

Таблиця 2

Відстань до джерела ПЭМВН	Значення норми відношення “небезпечний сигнал/шум”
5 м	1,7
10 м	1,5
15 м	1,4
20 м	1,3

Необхідно визначити ті напрямки розповсюдження небезпечного сигналу, щодо яких повинні бути застосовані атестовані засоби захисту від витоку каналами ПЕМВН.

9. Планується організувати обробку даних з грифом “цілком таємно” на персональному комп’ютері, навколо якого забезпечується контрольована територія. На межі цієї території виявлено побічне електромагнітне випромінювання, величина якого перевищує встановлені Норми. Представлений наступний список наявних засобів технічного захисту:

a) генератор просторового зашумлення;
b) генератор лінійного зашумлення;
c) завадозаглушувальний фільтр.

Необхідно вибрати засіб, який відповідає ситуації.

10. На якому етапі захисту за допомогою інструментального контролю визначається співвідношення небезпечний сигнал/шум, $P_{сиг}/P_{ш}$?

11. Планується організувати обробку даних з грифом “цілком таємно” на персональному комп’ютері, навколо якого забезпечується контрольована територія. На межі цієї території в телефонному проводі виявлено сигнал побічної електромагнітної наводки, величина якого перевищує встановлені норми. Представлений наступний список наявних засобів технічного захисту:

a) генератор просторового зашумлення.
b) засіб зашумлення системи електроживлення.
c) завадозаглушувальний фільтр.

Треба вибрати засіб, який відповідає ситуації.

12. Як можливо класифікувати загрози в ІКС?

13. Дайте визначення політиці безпеки інформації в ІКС. Основні компоненти її структури.

14. Як політика безпеки інформації в ІКС співвідноситься із правилами розподілу доступу (ПРД)?

15. Які основні компоненти політики безпеки інформації в ІКС?

16. Що таке ПРД? Основні формалізовані моделі розмежування доступу.

17. Дайте визначення термінам *інформаційний об’єкт, інформаційний суб’єкт, інформаційний процес.*

18. Яку модель політики доступу можливо описати за допомогою матриці доступу (access matrix)?

19. Сутність *мандатного управління доступом* (МП, Mandatory Access Control – MAC).

20. Сутність *рольової політики розподілу доступу* (РП, Role Base Access Control – RBAC).

21. Які напрямки захисту можуть бути реалізовані в рамках КСЗІ?

22. Який нормативний документ визначає порядок створення КСЗІ для ІКС, в яких обробляється інформація, яка є власністю держави, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством?

23. Перелічіть основні компоненти КСЗІ для ІКС, в яких обробляється інформація, яка належить до державної таємниці.

24. Які основні завдання підсистеми організаційного захисту КСЗІ?

25. Чим відрізняється інтегрована ІКС від ІКС?

26. Назвіть особливості створення КСЗІ для інтегрованої ІКС.

27. Яким чином оформлюється дозвіл на експлуатацію ІКС, яка обробляє інформації, що не становить державну таємницю?

28. Яким чином оформлюється дозвіл на експлуатацію ІКС, яка обробляє інформації, що становить державну таємницю?

8.2. Рейтингова система оцінювання результатів навчання.

Семестровий контрольний захід навчальної дисципліни передбачений у вигляді заліку. Шкала РСО навчальної дисципліни R дорівнює 100 балів ($R=100$). Рейтингові бали (RD) формуються як сума трьох складових:

1) $RD_k = \sum r_k$ – бали за семестрові контрольні заходи;

2) заохочувальні бали $RD_з = \sum r_з$;

3) штрафні бали $RD_ш = \sum r_ш$.

$$RD = RD_k + RD_з + RD_ш = \sum r_k + \sum r_з + \sum r_ш .$$

Якщо наприкінці семестру після проходження всіх контрольних заходів курсант отримав не менше 60 рейтингових балів ($60 \le RD$) , а також виконав умови допуску до семестрового контролю, він отримує позитивну оцінку.

Переведення рейтингових балів RD до оцінок за університетською шкалою здійснюється відповідно до табл. 4.

Таблиця 3 – Переведення рейтингових балів за університетською шкалою

Рейтингові бали, RD	Оцінка за університетською шкалою
$95 \le RD \le 100$	Відмінно
$85 \le RD \le 94$	Дуже добре
$75 \le RD \le 84$	Добре
$65 \le RD \le 74$	Задовільно
$60 \le RD \le 64$	Достатньо
$RD < 60$	Незадовільно

У разі, якщо сума рейтингових балів *RD* менша ніж 60, але виконані умови допуску до семестрової контролю (далі – необхідні додаткові умови допуску до залікової контрольної роботи), курсант виконує на останньому за розкладом занятті залікову контрольну роботу. За бажанням, курсант має право на участь у заліковій контрольній роботі з метою підвищення попередньої оцінки.

Рейтингові оцінки r_k, курсант отримує за виконання наступних контрольних заходів:

1) відповідь на поточні питання по змісту матеріалів занять (макс. значення – 40 балів);

2) результати виконання завдань поточних контрольних робіт (макс. значення – 40 балів);

3) результати підготовки матеріалів публічного захисту за завданнями самостійної роботи з мультимедійним супроводом (макс. значення – 20 балів).

В рамках цих контрольних заходів використовується наступна система балів та критеріїв оцінювання:

1) відповідь на поточні питання по змісту матеріалів занять оцінюється за чотирма оцінками – 0 (незадовільно), 3 (задовільно), 4 (добре), 5 (відмінно). Вага одної одиниці оцінки – 2 бали шкали *R.* Максимальна кількість опитувань – 4 (2 – лекції; 2 – ПЗ);

2) виконання завдань контрольних робіт також оцінюється чотирма оцінками – 0 (незадовільно), 3 (задовільно), 4 (добре), 5 (відмінно). Вага одної одиниці оцінки – 4 бали шкали *R.*

Критерії оцінювання відповідей на поточні питання та контрольні завдання наступні:

Критерії оцінювання відповідей на поточні питання та контрольні завдання	Оцінка
курсант показав глибоке знання предмету, правильно, обґрунтовано та повно сформулював відповідь, показав здатність вільно застосовувати професійну термінологію.	5
курсант показав знання предмету, правильно, обґрунтовано та повно сформулював відповідь, показав здатність застосовувати професійну термінологію. але була потрібна допомога викладача у вигляді додаткових питань.	4
курсант показав знання предмету, правильно, обґрунтовано та повно сформулював відповідь, але: – відповідь має недоліки непринципового характеру; – знання предмету є правильними, але неповними; – є недоліки у застосуванні професійних понять; – була потрібна допомога викладача у вигляді додаткових питань.	3
В інших випадках	0

3) підготовка матеріалів публічного захисту за завданнями самостійної роботи за чотирма оцінками – 0 (незадовільно), 3 (задовільно), 4 (добре), 5 (відмінно). Вага одної одиниці оцінки – 4 бали шкали *R*. Критерії оцінювання наступні:

Критерії оцінювання публічного захисту	Оцінка
Мета матеріалів чітко сформована та актуальна, зміст та структура відповідає меті, матеріал правильно і акуратно оформлений. Доповідь свідче про добри знання курсанта тематики самостійної роботи та відображає його здатність ефективно довести їх до аудиторії.	5
Мета матеріалів чітко сформована та актуальна, зміст та структура відповідає меті, матеріал правильно і акуратно оформлений. Доповідь свідче про добри знання курсанта. Є непринципові недоліки застосування методик та засобів доведення матеріалу до аудиторії. Була потрібна допомога викладача у вигляді поправок та додаткових питань.	4
Мета сформована, зміст та структура матеріалу відповідає меті не в повному обсязі, матеріал оформлений неохайно. Доповідь свідче про фрагментарні знання курсанта. Є недоліки застосування методик та засобів доведення матеріалу до аудиторії. Була потрібна допомога викладача у вигляді поправок та додаткових питань.	3
В інших випадках	0

Максимальне значення $RD_k=[(5\times2)\ \times4]+[(5\times4)\times2]+[(5\times4)\ \times1]=100$ *(балів)*

4) Заохочувальні бали $r_з$ (максимум – 10 балів) нараховуються за:

– активна робота на заняттях протягом семестру; – виконання завдань із удосконалення матеріально-технічної бази кафедри, дидактичних матеріалів з навчальної дисципліни.	до 3 балів
– підготовки комп'ютерного практикуму за індивідуальною темою; – участь у проведенні інноваційних або наукових досліджень курсантів.	до 10 балів

5) Штрафні бали $r_ш$ (максимум – 10 балів) нараховуються за:

– відсутність на практичному занятті без поважної причини; – незадовільна підготовка до практичного заняття; – неучасть в обговоренні доповідей курсантів за індивідуальною темою.	до 10 балів

Календарний контроль (атестація) здійснюється згідно Графіка-календаря освітнього процесу ІСЗЗІ КПІ м. Ігоря Сікорського на навчальний рік. Умовою атестації є отримання не менше ніж 50% від кількості балів, які курсант може отримати на час проведення атестації. В атестаційної відомості курсанту виставляється "атестовано" чи "неатестовано".

Курсанти, які набрали протягом семестру рейтинг з кредитного модуля менше 0,6 *R*, зобов'язані виконувати залікову контрольну роботу.

Курсанти, які набрали протягом семестру необхідну кількість балів ($RD \geq 0{,}6$ R), мають можливості:

– отримати залікову оцінку відповідно до набраного рейтингу;

– виконувати залікову контрольну роботу з метою підвищення оцінки;

– у разі отримання оцінки меншої, ніж попередній рейтинг *RD* курсанта, він отримує оцінку тільки за результатами залікової контрольної роботи.

Необхідні додаткові умови допуску до залікової контрольної роботи:

– отримано більше 23 балів за виконання завдань контрольних робіт;

– отримано більше 11 балів за виконання за підготовку матеріалів публічного захисту за завданнями самостійної роботи;

– отримано більше 11 балів за дві відповіді на поточні питання за змістом матеріалів занять.

Під час проведення залікової контрольної роботи визначається рівень засвоєння курсантом змісту навчання, сформованих знань, умінь і практичний досвід шляхом перевірки та оцінки рівня теоретичного та практичного матеріалу з певної навчальної дисципліни.

При визначенні оцінки курсанту до уваги беруться доповіді (обґрунтованість, чіткість, стислість), здатність впевнено та правильно відповідати на теоретичні питання і пояснювати практичні дії, здібність курсанта логічно побудувати свою відповідь, аргументовано відстоювати свою точку зору, наявність у курсанта методичних навичок.

Критерії оцінки відповіді курсанта (виконання контрольних завдань) мають враховувати, насамперед, її повноту і правильність, а також здатність курсанта:

1. Узагальнювати отримані знання.
2. Застосовувати правила, методи, принципи, закони в конкретних ситуаціях.
3. Аналізувати та оцінювати факти, події, інтерпретувати схеми, графіки, діаграми.
4. Викладати матеріал чітко, логічна, послідовно.

Результати складання залікової контрольної роботи оцінюються за наступною шкалою: “відмінно”, “дуже добре”, “добре”, “задовільно”, достатньо”, “незадовільно”.

При оцінюванні з відповідей курсантів необхідно орієнтуватися на такі загальні рекомендації.

“Відмінно” (95–100 балів) виставляється, якщо курсант демонструє повні й міцні знання навчального матеріалу в заданому обсязі, необхідний рівень умінь і навичок, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях.

“Дуже добре” (85–94 балів) – курсант демонструє повні й міцні знання навчального матеріалу в заданому обсязі, необхідний рівень умінь і навичок, допускає несуттєві неточності, має труднощі в трансформації умінь у нових умовах.

“Добре” (75–84 балів) – курсант демонструє знання навчального матеріалу в заданому обсязі, допускає несуттєві неточності логічного викладення матеріалу, має труднощі в трансформації умінь у нових умовах.

“Задовільно” (65–74 балів) – курсант засвоїв основний теоретичний матеріал, але допускає неточності, що не є перешкодою до подальшого навчання. Уміє використовувати знання для вирішення стандартних завдань.

“Достатньо” (60–64 балів) – курсант засвоїв основний теоретичний матеріал, але допускає неточності логічного викладення матеріалу, що не є перешкодою до подальшого навчання. В основному уміє використовувати знання для вирішення стандартних завдань.

“Незадовільно” (<60 балів) – незасвоєння окремих розділів, нездатність застосувати знання на практиці, що робить неможливим подальше навчання.

Рейтингова оцінка *RD* залікової контрольної роботи співвідноситься з традиційними оцінками згідно з табл. 2. У разі отримання курсантом незадовільної оцінки або наявності заборгованості, перескладання заліку з навчальної дисципліни допускається не більше двох разів. При другому перескладанні залік у курсанта може приймати комісія, яка створюється завідувачем спеціальної кафедри. Оцінка, отримана курсантом у результаті другого перескладання заліку, є остаточною.

9. Додаткова інформація з навчальної дисципліни

Перелік питань, які виносяться на семестровий контроль:

1. Класифікація інформаційних (автоматизованих) систем і функціональні профілі захищеності від НСД.
2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НСД).
3. Порядок визначення стандартного функціонального профілю захищеності.
4. Порядок визначення засобів захисту від НСД.
5. Організація робіт по забезпеченню інформації від витоку каналами ПЕМВН.
6. Проведення обстеження засобів ЕОТ.
7. Концептуальна модель кіберпростору, кібербезпека, критерії кібербезпеки.
8. Структура корпоративної IT-системи.

9. Архітектура захисту корпоративної IT-системи. Інтернет модуль корпоративної IT-системи: структура, заходи і засоби захисту.
10. Кампусний модуль корпоративної IT-системи: структура, заходи і засоби захисту.
11. IDS/IPS: призначення, принципи роботи, варіанти застосування в корпоративної IT-системі.
12. База кіберзагроз MITRE ATT&CK.
13. Аудит та оцінка безпеки комп'ютерних систем: базові терміни та сутність.
14. Модель (ІФС) процесу аудиту і оцінки безпеки IT-системи.
15. Концепція аудиту і оцінки безпеки ITS.
16. Тестування на проникнення: призначення, порядок проведення, основні параметри тестування.
17. Кібернетична модель проактивного кіберзахисту (24/7).
18. SOC: призначення, основні процеси.
19. SIEM: призначення, основні процеси.
20. Cyber threat intelligence: призначення, основні процеси.
21. Загрози та основні вразливості Exeution through Module Load.
22. Загрози на основі вразливості Rundll32.
23. Загрози на основі вразливості XLS Script Processing.
24. Загрози на основі вразливості Bits Jobs.
25. Загрози на основі вразливості CMSTP.
26. Загрози на основі вразливості User Execution.
27. Загрози та основні вразливості Windows Remote Management.
28. Загрози на основі вразливості Execution through API.
29. Загрози на основі вразливості Remote file copy.
30. APT атаки: сутність та порядок визначення.
31. APT атаки: моделі і порядок їх застосування.
32. Кібернетична модель APT атаки.
33. Модель "Cyber kill chain".