МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДОНБАСЬКА ДЕРЖАВНА МАШИНОБУДІВНА АКАДЕМІЯ

Кафедра «Автоматизація виробничих процесів»

"ЗАТВЕРДЖУЮ"
Ректор ДДМА

_____ В.Д.Ковальов

"04" 09 2020 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

„ ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ "

(назва дисципліни)

Галузь знань: 12 «Інформаційні технології»

Спеціальність 123 «Комп'ютерна інженерія"

Освітній рівень – перший (бакалаврський)

ОПП «Комп'ютерні системи та мережі»

Факультет «Машинобудування»

(назва інституту, факультету, відділення)

КРАМАТОРСЬК, 2020

Робоча програма навчальної дисципліни «Захист інформації в комп'ютерних системах» для студентів галузі знань 12 «Інформаційні технології» спеціальності 123 «Комп'ютерна інженерія».

Розробник: **Костіков О.А.**, канд. фіз.-мат. наук, доц.

Погоджено з групою забезпечення освітньої програми (для обов'язкових дисциплін).

Керівник групи забезпечення: _____ О.В. Суботін, к.т.н., доцент

Розглянуто і затверджено на засіданні кафедри «Автоматизація виробничих процесів», протокол № 10 від 22.06.2020 року.

Завідувач кафедри АВП: _____ Г.П. Клименко, д.т.н., професор

Розглянуто і затверджено на засіданні Вченої ради факультету машинобудування, протокол № 01-20/08 від 31.08.2020 року.

Голова Вченої ради факультету: _____ В.Д. Кассов, д.т.н., професор

1.Опис навчальної дисципліни

<table>
<tr><td colspan="2" rowspan="2">Показники</td><td rowspan="2">Галузь знань, спеціальність, ОПП (ОНП), професійне (наукове) спрямування, рівень вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна</td><td>прискорена</td></tr>
<tr><td colspan="2">Кількість кредитів</td><td rowspan="4">Галузь знань:
12 «Інформаційні технології».
Спеціальність:
123 «Комп’ютерна інженерія».
ОПП
«Комп’ютерні системи та мережі»</td><td colspan="2" rowspan="4">Обов’язкова дисципліна</td></tr>
<tr><td>7</td><td>3</td></tr>
<tr><td colspan="2">Загальна кількість годин</td></tr>
<tr><td>210</td><td>90</td></tr>
<tr><td colspan="2">Модулів – 2</td><td rowspan="4"></td><td colspan="2">Рік підготовки</td></tr>
<tr><td colspan="2">Змістових модулів –2</td><td>4</td><td>2</td></tr>
<tr><td colspan="2" rowspan="2">Індивідуальне науково-дослідне завдання _ Побудова прототипу експертної системи</td><td colspan="2">Семестр</td></tr>
<tr><td>8</td><td>4</td></tr>
<tr><td colspan="2" rowspan="10">Тижневих годин
для денної форми навчання:
аудиторних – 8;
самостійної роботи студента – 8</td><td rowspan="10">Рівень вищої освіти:
перший (бакалаврський)</td><td colspan="2">Лекції</td></tr>
<tr><td>56</td><td>26</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>26</td><td>26</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>26</td><td></td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>102</td><td>38</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td>екзамен</td><td>екзамен</td></tr>
</table>

2. ЗАГАЛЬНІ ВІДОМОСТІ, МЕТА І ЗАВДАННЯ ДИСЦИПЛІНИ

Мета дисципліни – формування у майбутніх фахівців сучасного рівня культури з інформаційної безпеки, а також набуття практичних навичок з основ застосування сучасних методів забезпечення захисту інформації в комп'ютерних системах.

Завдання дисципліни - надання основних відомостей з принципів протидії спробам несанкціонованого доступу до інформації з боку сторонніх осіб; придбання знань в області захисту інформації в комп'ютерних системах та мережах; освоєння засобів аналізу погроз інформації; вивчення принципів використання основних методів, алгоритмів та засобів здійснення захисту інформації у системах та мережах.

Програмні компетентності. Освітня компонента «Захист інформації в комп'ютерних системах» повинна сформувати наступні загальні та фахові програмні компетентності, що передбачені освітньо-професійною програмою підготовки бакалаврів «Комп'ютерні системи та мережі»:

ЗК1. Здатність до абстрактного мислення, аналізу і синтезу.

ЗК2. Здатність вчитися і оволодівати сучасними знаннями.

ЗК3. Здатність застосовувати знання у практичних ситуаціях.

ФК3. Здатність створювати системне та прикладне програмне забезпечення комп'ютерних систем та мереж.

ФК4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

ФК10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

Програмні результати навчання. Освітня компонента «Системне програмне забезпечення» повинна сформувати наступні програмні результати навчання, що передбачені освітньо-професійною програмою підготовки бакалаврів «Комп'ютерні системи та мережі»:

ПР1. Знати та розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

ПР3. Знати новітні технології в галузі комп'ютерної інженерії.

ПР7. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

ПР15. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів.

Передумови для вивчення дисципліни:

Комп'ютерні технології та програмування.

Мова викладання: українська.

Обсяг навчальної дисципліни та його розподіл за видами навчальних занять:

- загальний обсяг для денної форми навчання становить 210 годин/ 7 кредити, в тому числі: лекції - 56 годин, лабораторні роботи – 26 годин, практичні заняття - 26 годин, самостійна робота студентів - 102 години;
- загальний обсяг для прискореної форми навчання становить 90 годин/ 3 кредити, в тому числі: лекції 26 годин, лабораторні роботи - 26 годин, самостійна робота студентів - 38 годин.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1.
Концепції забезпечення інформаційної безпеки, захист віддаленого доступу, VPN, безпечна маршрутизація і комутація

Тема 1. Концепції забезпечення інформаційної безпеки.

Лекція 1. Принципи забезпечення безпеки в комп'ютерних системах.

Загальні поняття захисту інформації. Важливість проблеми захисту інформації. Закони України про захист інформації. Цілі інформаційної безпеки. Управління інформацією про безпеку та події(SIEM). Визначення, що використовуються в сфері інформаційної безпеки. Зони безпеки мережі.

Лекція 2. Загрози інформаційній безпеці.

Розвідка. Атака соціальної інженерії. Ескалація пільг. Мережеві загрози. Зловмисне програмне забезпечення. Втрата даних(ексфільтрація).

Лекція 3. Криптографічний захист інформації.

Основні поняття криптографічного захисту інформації. Симетричні криптосистеми шифрування. Асиметричні криптосистеми шифрування. Функції хешування. Електронний цифровий підпис. Управління криптоключами. Інфраструктура управління відкритими ключами PKI.

Тема 2. Захист віддаленого доступу.

Лекція 4. Безпечне управління. Захист площини управління (MPP). Надійні рекомендації щодо паролів. Блокування після невдалого входу. Автентифікація користувача. Рольовий контроль доступу (RBAC). Зашифровані протоколи для віддаленого доступу.

Лекція 5. Концепції організації автентифікації, авторизації та аудиту(AAA).

Поняття автентифікації, авторизації та аудиту Контроль доступу до інфраструктури. Протоколи AAA. Cisco Identity Services Engine(Cisco ISE). Налагодження TACAS+. Налагодження RADIUS автентифікації.

Тема 3. Технології віртуальних приватних мереж VPN.

Лекція 6. Концепція побудови віртуальних приватних мереж VPN.

Основні поняття і функції мережі VPN. Переваги використання VPN. Типи VPN. Варіанти побудови віртуальних захищених каналів. Забезпечення безпеки VPN.

Лекція 7. Протокол IPSec.

Робота протоколу IPsec. Захист рівня IP за допомогою IPsec. Набори перетворень. Режими роботи IPsec.

Лекція 8. Протокол SSL VPN.

SSL і TLS для безпечного зв'язку. Робота SSL і TLS. Параметри реалізації VPN на основі SSL. Порівняння між SSL та IPsec.

Тема 4. Безпечна маршрутизація і комутація.

Лекція 9. Забезпечення безпеки в маршрутизаторах Cisco. Безпечні протоколи маршрутизації.

Функція стійкої конфігурації Cisco IOS. Відновлення архівованої конфігурації. Проблеми безпеки, пов'язані з динамічною маршрутизацією. Забезпечення безпеки площини управління.

Лекція 10. Розповсюджені атаки 2-го рівня.

Атака STP. ARP спуфінг. Спуфінг / копіювання MAC. Розвідка CDP / LLDP. Перестрибування VLAN. DHCP спуфінг.

Лекція 11. Процедури подавлення атак.

DHCP снупінг. Особливості снупінгу. Захист порту. Протокол відкриття. BPDU Guard. Root Guard. Loop Guard.

Змістовий модуль 2
Технології міжмережевого екранування, IPS, безпека контенту та кінцевих точок.

Тема 5. Технології міжмережевого екранування.

Лекція 12. Брандмауер.

Архітектура брандмауера. Типи брандмауера. Зауваження щодо розгортання та проектування брандмауерів. Порівняння stateful та ststeless брандмауерів. Списки контролю доступу (ACL).

Лекція 13. Технологія Cisco IOS Zone Based Firewall.

Мова застосування політик C3HL(Cisco Common Classification Policy Language). Складові компоненти C3PL. Self Zone. Правила поведінки між зонами за замовчанням.

Лекція 14. Багатофункціональний пристрій захисту Cisco Adaptive Security Appliance (ASA).

Управління доступом ASA. Політика безпеки доступу. Рівні безпеки ASA. Фреймворк модульної політики Cisco (MPF). Режими розгортання. Методи реалізації високої доступності. Контекст безпеки. Функції брандмауера.

Лекція 15. Реалізація NAT в Cisco ASA.

Статичний NAT. Дінамічний NAT. PAT.Політика NAT. Перевірка NAT операцій.

Тема 6. Система запобігання вторгнень (IPS).

Лекція 16. Огляд систем виявлення та запобігання вторгненням (IDS/IPS).

Параметри інтеграції IPS / IDS. Методи розгортання IDS / IPS. Режими розгортання. Розміщення пристрою IDS / IPS. IDS / IPS технології.

Лекція 17. Виявлення зловмисного трафіку.

Сигнатури IDS / IPS. Управління та розгортання сигнатур. Сигнатурний метод виявлення зловмисного трафіку. Метод аномалій. Метод політик.

Лекція 18. Сенсори IDS/IPS.

Реакція сенсорів на зловмисний трафік. Управління поведінкою IDS/IPS сенсорів. Подолання IDS/IPS модуля. Дії та реакції тригерів.

Тема 7. Безпека контенту та кінцевих точок.

Лекція 19. Технологія запобігання погроз на основі електронної пошти.

Пристрій захисту електронної пошти Cisco (ESA). Рішення Cisco щодо хмарної та гібридної електронної пошти. Розширений захист від шкідливих програм. Запобігання втраті даних електронною поштою (DLP). Внесення в чорний список. Шифрування електронної пошти. Цифровий підпис. Використання протоколів SSL і TLS для безпечного зв'язку.

Лекція 20. Технологія запобігання веб-загрозам.

Хмарна веб-безпека (CWS). Пристрій веб-безпеки Cisco (WSA). Фільтрування URL-адрес. Фільтрування веб-додатків. Брандмауер веб-додатків. Сканування шкідливого програмного забезпечення. Дешифрування інтернет трафіку, зашифрованого за допомогою TLS / SSL. Пристрій управління безпекою контенту Cisco (Cisco Content Security Management Appliance).

Лекція 21. Технології захисту кінцевих точок. Антивірусний захист.

Поняття комп'ютерного віруса. Віруси та „трояни", визначення та класифікація. Модель вірусу та модель „трояна". Класифікація комп'ютерних вірусів. Засоби розповсюдження. Негативні наслідки дії вірусних програм. Захист операційних систем від програм-закладок. Програми „кілогери"-"клавіатурні шпигуни", визначення та класифікація. Налагодження антикілогерів. Антивірусне програмне забезпечення Профілактика вірусного зараження. Антивірусні монітори та сканери. Налаштування антивірусних засобів.

Лекція 22. Технології захисту кінцевих точок. Брандмауери, HIPS, AMP.

Персональні брандмауери та системи запобігання вторгненню (HIPS). Поліпшений захист від шкідливих програм (AMP) для кінцевих точок. Апаратне та програмне шифрування даних кінцевих точок.

Лекція 23. Безпека операційних систем.

Загрози безпеки операційної системи. Поняття захищеної операційної системи. Архітектура підсистеми захисту операційної системи. Основні функції підсистеми захисту операційної системи. Ідентифікація, аутеніфікація, та авторизація суб’єктів доступу. Розмежування доступу до об’єктів операційної системи.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

4.1. Розподіл обсягу дисципліни за видами навчальних занять та темами .

Для денної форми навчання

№ з/п	Назви змістових модулів і тем	Кількість годин				
		Усього	в т.ч.			
			Л	П (С)	Лаб	СРС
Змістовий модуль 1. Концепції забезпечення інформаційної безпеки, захист віддаленого доступу, VPN, безпечна маршрутизація і комутація.						
1	Тема 1. Концепції забезпечення інформаційної безпеки.	30	6	10		14
2	Тема 2. Захист віддаленого доступу.	24	4	2	4	14
3	Тема 3. Технології віртуальних приватних мереж VPN.	27	9		4	14
4	Тема 4. Безпечна маршрутизація і комутація.	31	9	2	6	14
Змістовий модуль 2. Технології міжмережевого екранування, IPS, безпека контенту та кінцевих точок.						
5	Тема 5. Технології межмережевого екранування.	32	10	2	6	14
6	Тема 6. Система запобігання вторгнень(IPS).	31	9	2	6	14
7	Тема 7. Безпека контенту та кінцевих точок.	35	9	8		18
	Усього годин	**210**	**56**	**26**	**26**	**102**

Для денної прискореної форми навчання

№ з/п	Назви змістових модулів і тем	Кількість годин				
		Усього	в т.ч.			
			Л	П (С)	Лаб	СРС
Змістовий модуль 1 Концепції забезпечення інформаційної безпеки, захист віддаленого доступу, VPN, безпечна маршрутизація і комутація.						
1	Тема 1. Концепції забезпечення інформаційної безпеки.	7	2			5
2	Тема 2. Захист віддаленого доступу.	11	2		4	5
3	Тема 3. Технології віртуальних приватних мереж VPN.	13	4		4	5
4	Тема 4. Безпечна маршрутизація і комутація.	15	4		6	5

№ з/п	Назви змістових модулів і тем	Кількість годин				
		Усього	в т.ч.			
			Л	П (С)	Лаб	СРС
Змістовий модуль 2 Технології міжмережевого екранування, IPS, безпека контенту та кінцевих точок.						
5	Тема 5. Технології межмережевого екранування.	17	6		6	5
6	Тема 6. Система запобігання вторгнень(IPS).	15	4		6	5
7	Тема 7. Безпека контенту та кінцевих точок.	12	4			8
	Усього годин	**90**	**26**		**26**	**38**

Л – лекції, П (С) – практичні (семінарські) заняття, Лаб – лабораторні заняття, СРС – самостійна робота студентів.

5. ТЕМИ ЛАБОРАТОРНИХ РОБІТ

№ з/п	Тема	Назва лабораторної роботи	Кількість годин
Змістовий модуль 1 Концепції забезпечення інформаційної безпеки, захист віддаленого доступу, VPN, безпечна маршрутизація і комутація.			
1	Тема 2	AAA-сервер	2
2	Тема 2	Надання доступу по AAA.	2
3	Тема 3	VPN за допомогою IPSec.	2
4	Тема 3	Віртуальна приватна мережа VPN.	2
5	Тема 4	Безпека маршрутизатора	2
6	Тема 4	Аутеніфікація в протоколі динамічної маршрутизації.	2
7	Тема 4	Налагодження Port Security	2
Змістовий модуль 2 Технології міжмережевого екранування, IPS, безпека контенту та кінцевих точок.			
8	Тема 5	Списки доступу.	2
9	Тема 5	Налагодження Zone-Based Firewall.	2
10	Тема 5	Налагодження безпечної мережі за допомогою Cisco ASA(Adaptive Security Appliance).	2
11	Тема 6	Налагодження комплексу Cisco IDS Sensor.	3
12	Тема 6	Виявлення комп’ютерних атак на вузли мережі за допомогою Cisco IDS Sensor.	3
		Усього годин	**26**

6. ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Тема	Назва лабораторної роботи	Кількість годин
Змістовий модуль 1 Концепції забезпечення інформаційної безпеки, захист віддаленого доступу, VPN, безпечна маршрутизація і комутація.			
1	Тема 1	Мережеві загрози	2
2	Тема 1	DDOS-атаки	2
3	Тема 1	Шифрування методом гамування	2
4	Тема 1	Шифрування методом RSA	2
5	Тема 1	Шифрування за допомогою алгоритма DES	2
6	Тема 2	Локальна аутеніфікація AAA	2
7	Тема 4	Захист мережевих пристроїв	2
Змістовий модуль 2 Технології міжмережевого екранування, IPS, безпека контенту та кінцевих точок.			
8	Тема 5	Вивчення можливостей брандмауера iptables	2
9	Тема 6	Впровадження запобігання вторгнень	2
10	Тема 7	Вивчення комплексу захисту ОС Windows	2
11	Тема 7	Вивчення засобів захисту Active Directory	3
12	Тема 7	Установка та налагодження антивірусного комплексу	3
		Усього годин	**26**

7. САМОСТІЙНА РОБОТА

№ з/п	Зміст самостійної роботи студента	Кількість годин
1	Хмарні і віртуальні мережі	10
2	Політика безпеки мережі	10
3	Framework NFP	10
4	Призначення адміністративних ролей	10
5	Використання SNMP і NTP	10
6	Підписи і впровадження IPS	10
7	Безпека 2-го рівня	10
8	Конфіденційність і шифрування	10
9	Криптографія відкритого ключа	10
10	Впровадження VPN-сайтів; IPsec-сайтів; сайтів з CLI.	12
Разом		**102**

7. МЕТОДИ НАВЧАННЯ

В навчальному процесі застосовуються: лекції з використанням мультимедіа матеріалів; практичні(лабораторні) роботи в комп'ютерному класі з пошуком інформації в Інтернет та самостійна робота.

8. МЕТОДИ КОНТРОЛЮ

При вивченні дисципліни використовуються наступні методи контролю: проведення поточного контролю, письмового підсумкового контролю у вигляді екзамену, модульного контролю.

Захист практичних(лабораторних) робіт показує рівень теоретичного і практичного засвоєння матеріалу і слугує поточним контролем рівня підготовки студента. Розподіл балів, що отримують студенти, наведено в розділі 11.

Основним засобом контролю є модульна контрольна робота. Під час їх виконання студент показує повноту засвоєння матеріалу та вміння використовувати свої знання. Тематика модульних контрольних робіт наведена в розділі 10.

9. КОНТРОЛЬНІ РОБОТИ

Контрольні роботи з теоретичної частини розподілені таким чином:

№ роботи	№ теми	Тема контрольної роботи	Кількість варіантів
		1-й семестр	
1	1-4	Склад СПЗ та інструментарій його розробки..	20
2	5-7	Розробка СПЗ.	20

10. КРИТЕРІЇ ОЦІНЮВАННЯ ТА РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ

10.1 Розподіл балів, що отримують студенти (кількісне оцінювання):

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1			
Виконання і захист лабораторних і практичних завдань	0...7	5	0...35
Модульний контроль	0...20	1	0...20

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 2			
Виконання і захист лабораторних і практичних завдань	0...6	5	0...30
Модульний контроль	0...15	1	0...15
Усього			**55... 100**

10.2 Критерії оцінки знань студентів протягом семестру

Критерії оцінювання практичних(лабораторних) робіт

Вимоги	Кількість балів
Завдання відзначається повнотою виконання без допомоги викладача. Визначає рівень поінформованості, потрібний для прийняття рішень. Вибирає інформаційні джерела. Робить висновки і приймає рішення у ситуації невизначеності. Володіє уміннями творчо-пошукової діяльності.	5
Завдання - повні, з деякими огріхами, виконані без допомоги викладача. Планує інформаційний пошук: володіє способами систематизації інформації. Студент може зіставити, узагальнити, систематизувати інформацію під керівництвом викладача: вільно застосовує вивчений матеріал у стандартних ситуаціях. Робить висновки і приймає рішення у ситуації невизначеності. Володіє уміннями творчо-пошукової діяльності.	3-4
Завдання відзначається неповнотою виконання за консультацією викладача. Застосовує запропонований викладачем спосіб отримання інформації, має фрагментарні навички в роботі з підручником, науковими джерелами: Вибирає відомі способи дій для виконання фахових методичних завдань.	1-2

Критерії оцінювання модульних контрольних робіт

18-20(13-15) балів виставляється, коли студент дає абсолютно правильні відповіді на теоретичні питання з викладенням оригінальних висновків, отриманих на основі програмного, додаткового матеріалу та нормативних документів. При виконанні практичного завдання студент застосовує системні знання навчального матеріалу, передбачені навчальною програмою.

16-17(12) балів виставляється студенту, який повністю розкрив теоретичні питання на основі програмного та додаткового матеріалу. При виконанні практичних завдань студент застосовує узагальнені знання навчального матеріалу, передбачені навчальною програмою.

13-15(10-11) балів виставляється студенту, який повністю розкрив теоретичні питання, а програмний матеріал викладено у відповідності до вимог. Практичні завдання виконані в цілому правильно, але мають місце окремі неточності.

10-12(8-10) балів виставляється, коли студент розкрив теоретичні питання, проте при викладенні програмного матеріалу допущені окремі помилки. При виконанні практичних завдань студент припускається помилок, за рахунок недостатнього розуміння програмного матеріалу.

7-9(5-7) балів виставляється, коли студент неповністю розкрив теоретичні питання, відповідь містить суттєві помилки. При виконанні практичних завдань студент припускається значних помилок, а виконання завдань викликає значні труднощі у студента.

4-6(3-4) бали виставляються студенту, який не розкрив теоретичні питання і не може виконати практичні завдання. Як правило такий студент виявляє здатність до викладення думки лише на елементарному рівні.

0-3(0-2) бали виставляється студенту, який не виконав навчальну програму або якийсь елемент її складової, має фрагментарні знання, які не дозволяють розкрити теоретичні питання і виконати практичні завдання. Такий студент не може викласти свою думку навіть на елементарному рівні.

10.3 Підсумкова оцінка за семестр

Контроль знань здобувачів здійснюється за рейтинговою накопичувальною (100-бальною) системою, яка передбачає складання обов’язкових контрольних точок.

Підсумкова оцінка за дисципліну складається з оцінки, отриманої на протязі семестру, та оцінки, отриманої на екзамені.

Після завершення семестру проводиться семестровий екзамен, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Максимальна кількість балів (100) при оцінюванні знань з навчальної дисципліни, яка завершується екзаменом, формується з двох частин, з коефіцієнтом 0,5 кожна:

– за поточну успішність 100 балів (сума балів, зароблена у семестрі, але не менше 55);

– на екзамені 100балів (мінімально необхідна кількість балів за екзамен 55).

Підсумкові оцінки за триместр в цілому переводяться за національною шкалою та шкалою ECTS відповідно до таблиці переводу, яка визначається діючим в ДДМА положення про організацію навчального процесу в кредитно-модульній системі підготовки фахівців:

Рейтингова оцінка	**У національній шкалі**	**У шкалі ECTS**
90-100	Відмінно (зараховано)	A
81-89	Добре (зараховано)	B
75-80	Добре(зараховано)	C
65-74	Задовільно (зараховано)	D
55-64	Задовільно (зараховано)	E
30-54	Незадовільно (не зараховано)	FX
0-29	Незадовільно (не зараховано)	F

Для отримання позитивної оцінки з дисципліни студент повинен одержати не менше ніж 55 балів сумарної оцінки.

11. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ

1. Захист інформації в комп’ютерних системах. Конспект лекцій (для студентів спеціальності 123 «Комп’ютерна інженерія»).

2. Методичні вказівки до виконання практичних(лабораторних) робіт з дисципліни ”Захист інформації в комп’ютерних системах” (для студентів спеціальності 123 «Комп’ютерна інженерія»).

12. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Література основна

1. Omar Santos. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide. - Cisco Press, 2020. – 1635p.

2. CCNA Security (IINS 210-260) Complete Training Guide With Practice Exam Questions, 2nd Ed. - IPSpecialist LTD, 2019. – 513p.

3. Daimi, Kevin. Computer and Network Security Essentials. – Springer, 2018. – 609p.

4. Singh Glen, Vinod Michael, Anandh Vijay. CCNA Security 210-260 Certification Guide: Build your knowledge of network security and pass your CCNA Security exam (210-260). - Packt Publishing, 2018. – 518p.

5. McMillan, Troy. CCNA security study guide: exam 210-260. – Sybex, 2018. – 358p

6. William Stallings. Cryptography and Network Security: Principles and Practice, Global Edition. - Pearson, 2017. – 768p.

7. Бобало Ю.Я., Горбатий І.В. та ін. Інформаційна безпека. – Львівська політехніка, 2019. – 580 с.

8. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації. – Родовід, 2014. – 428 с.

9. Олифер Виктор, Олифер Наталья. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. — СПб.: Питер, 2020. — 1008с.

10. Шаньгин В. Ф. Информационная безопасность и защита информации -Эл. изд. Саратов: Профобразование, 2017 - 702 с.

Література додаткова

1. Omar Santos, Panos Kampanakis, Aaron Woland. Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP. - Cisco Press, 2016. – 368p.

2. Bob Vachon. CCNA Security (210-260) Portable Command Guide (2nd Edition). - Cisco Press, 2016. – 352p.

3. Решения компании Cisco Systems по обеспечению безопасности корпоративных сетей (издание II). – 2006. – 100 с.

4. Хорев П. Б.Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений. — М.: Издательский центр «Академия», 2005. — 256 с.

5. Уэнстром М. Организация зашиты сетей Cisco.: Пер. с англ. — М. : Издательский дом "Вильямс", 2005. —768 с.

Інформаційні ресурси в мережі Інтернет

1. Журнал "Информаційні технології. Аналітичні матеріали" [Электронный ресурс]. – Режим доступа : http://it.ridne.net.

2. Нормативные акты Украины [Электронный ресурс]. – Режим доступа : www.nau.kiev.ua.

3. Information Technology Security Evaluation Criteria, v. 1.2. – Office for Official publications of the European Communities, 1991 [Electronic resource]. – Access mode : www.fbi.gov.

4. https://www.cisco.com/c/ru_ua/index.html

5. https://www.netacad.com/front

6. https://www.cisco.com/c/ru_ru/products/security/index.html

Додаток А

Питання для підготовки до контрольної роботи та екзамену з дисципліни «Захист інформації в комп'ютерних мережах»

1. Визначення інформаційній безпеки.
2. Об'єкти інформаційної безпеки.
3. Інтереси держави в інформаційній сфері.
4. Аналіз даних захисту.
5. Право інтелектуальної власності та політика інформаційної безпеки.
6. Управління безпекою.
7. Розробка правил безпеки.
8. Зміст моделі системи захисту інформації.
9. Основні принципи та рівні захисту інформаційних систем
10. Моделі і системи шифрування.
11. Класифікація криптографічних методів.
12. Визначення «цифрового підпису».
13. Складові безпеки інформаційної системи і відповідні специфікації функцій безпеки.
14. Аутентифікація та безпека мережі.
15. Правила використання електронної пошти.
16. Використання електронної пошти для конфіденційного обміну інформацією
17. Програми виявлення вірусів та заходи по захисту та профілактиці
18. Антивірусні пакети
19. Дія троянських програм.
20. Яка основна відмінність між вірусом та хробаком?
21. Класифікація комп'ютерних вірусів.
22. Ознаки класифікації комп'ютерних вірусів.
23. Методи та засоби захисту програмного забезпечення.
24. Класифікація засобів захисту програмного забезпечення.
25. Безпека граничного маршрутизатора
26. Налагодження безпечного адміністративного доступу
27. Характеристики AAA
28. Налаштування локальної AAA аутентифікації з використанням CLI.
29. Характеристики серверних AAA
30. Протоколи зв'язку серверних AAA
31. Технології VPN
32. Протоколи безпеки IPSec
33. Налаштування Site-to-site IPSec VPN.
34. Налаштування сумісних ACL.
35. Основи налаштування ASA.
36. Служби NAT на основі ASA.
37. Політики служб на основі ASA.
38. SSL VPNs.

39. Функціонування зональної політики брандмауера.
40. Налаштування зональної політики брандмауера з використанням CLI.
41. Характеристики IDS і IPS.
42. Реалізації мережевої (Network-based) IPS
43. Налаштування Cisco IOS IPS з використанням CLI.
44. Характеристики IPS підпису.
45. Дії IPS підпису.
46. Безпека 2-го рівня.
47. Атаки з підміною MAC адрес.
48. Атаки з маніпуляцією STP.
49. Налаштування Port security.