Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«05» 09 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Протокол № 0134/22
(підпис) (прізвище, ініціали)
«___» 2022

2022 – 2023 навчальний рік

Розробник:

Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____(підпис)_____ Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.

Керівник освітньої програми _____(підпис)_____ Артем ПЛАТОНЕНКО

Робочу програму перевірено

___.___. 2022 р.

Заступник декана _____(підпис)_____ Євген ІВАНІЧЕНКО

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання		
	денна		заочна
Вид дисципліни	обов'язкова		
Мова викладання, навчання та оцінювання	українська		
Загальний обсяг кредитів / годин	10 / 300		
Курс	2	3	
Семестр	4	5	
Кількість змістових модулів з розподілом:	8		
Обсяг кредитів	6	4	
Обсяг годин, в тому числі:	180	120	
Аудиторні	84	28	
Модульний контроль	12	4	
Семестровий контроль	-	60	
Самостійна робота	84	28	
Форма семестрового контролю	залік	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Захист інформації в інформаційно-комунікаційних системах» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека, освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Захист інформації в інформаційно-комунікаційних системах» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Захист інформації в інформаційно-комунікаційних системах» складається з восьми змістових модулів: Технології забезпечення безпеки мережевої інфраструктури; Захист трафіку за технологією VLAN та тунелювання; Визначення вихідних даних щодо створення КСЗІ в ІТС; Формування політики безпеки інформації в ІТС; Системи запобігання витоку інформації; Системи виявлення запобігання вторгненням; Управління доступом в мережі. Захисту електронної пошти; Забезпечення безпеки інформації в корпоративних мережах. Обсяг дисципліни – 300 год. (10 кредитів).

Метою викладання навчальної дисципліни «Захист інформації в інформаційно-комунікаційних системах» є формування у студентів уміння вирішувати задачі аналізу середовищ функціонування програмних та програмно-апаратних комплексів в інформаційно-телекомунікаційних (автоматизованих) системах, формування політики безпеки інформації в ІТС, застосовувати нормативно-правові, організаційні та технічні процедури забезпечення безпеки інформації в корпоративних мережах.

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері

інформаційної та кібернетичної безпеки та набуття **наступних фахових компетентностей**:

КФ-3: Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) та *SMART* системах.

КФ-5: Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) та *SMART* системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ-7: Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати:

- процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем від порушників безпеки інформації;
- методи та види несанкціонованого доступу та канали витоку інформації в інформаційно-телекомунікаційних (автоматизованих) системах;
- методику визначення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних та автоматизованих системах;
- принципи протидії несанкціонованому доступу до ресурсів і процесів в ІТС;
- функції та особливості реалізації системи захисту інформації в інформаційних, інформаційно-телекомунікаційних та автоматизованих системах.

уміти:

- аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних;
- застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектури операційних систем;
- виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної та/або кібербезпеки в ІТС;
- вирішувати задачі підготовки вихідних даних до проектування комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
- здійснювати оцінку рівня захищеності інформації що обробляється в ІТС та оцінки наявності потенційних вразливостей.

та досягти наступних **програмних результатів навчання:**

ПРз-2: здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних та *SMART* технологій; розробляти та аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектури операційних систем; здійснювати захист ресурсів і процесів в ІТС на основі моделей безпеки, а також встановлених режимів безпечного функціонування ІТС; виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної та/або кібербезпеки в ІТС.

ПРз-3: забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) та *SMART* систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

ПРз-7: вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART* системах; здійснювати оцінку

рівня захищеності інформації що обробляється в ІТС використовувати інструментальні засоби оцінювання наявності потенційних вразливостей; вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих); вирішувати задачі експертизи, випробування КСЗІ.

ПРз-11: забезпечувати процеси моніторингу доступу до ресурсів і процесів ІТ та *SMART* системах; забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в ІТС.

ПРз-12: виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних та автоматизованих системах; аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в ІТ та *SMART* системах; аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
СЕМЕСТР 4							
Змістовий модуль 1. Технології забезпечення безпеки мережевої інфраструктури							
Тема 1. Технології забезпечення безпеки мережевої інфраструктури	28	6		4	4		14
Модульний контроль	2						
Разом	30	6		4	4		14
Змістовий модуль 2. Захист трафіку за технологією VLAN та тунелювання							
Тема 2. Захист трафіку за технологією VLAN та тунелювання	28	4		4	6		14
Модульний контроль	2						
Разом	30	4		4	6		14
Змістовий модуль 3. Визначення вихідних даних щодо створення КСЗІ в ІТС							
Тема 3. Визначення вихідних даних щодо створення КСЗІ в ІТС	28	4		6	4		14
Модульний контроль	2						
Разом	30	4		6	4		14
Змістовий модуль 4. Формування політики безпеки інформації в ІТС							
Тема 4. Формування політики безпеки інформації в ІТС	28	6		4	4		14
Модульний контроль	2						
Разом	30	6		4	4		14

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 5. Системи запобігання витоку інформації							
Тема 5. Системи запобігання витоку інформації	28	4		4	6		14
Модульний контроль	2						
Разом	30	4		4	6		14
Змістовий модуль 6. Системи виявлення запобігання вторгненням							
Тема 6. Системи виявлення запобігання вторгненням	28	4		6	4		14
Модульний контроль	2						
Разом	30	4		6	4		14
СЕМЕСТР 5							
Змістовий модуль 7. **Управління доступом в мережі. Захист електронної пошти**							
Тема 7. Управління доступом в мережі для базових операційних систем	14	2		2	2		8
Тема 8. Механізми захисту електронної пошти	14	2		2	4		6
Модульний контроль	2						
Разом	30	4		4	6		14
Змістовий модуль 8. Забезпечення безпеки інформації в корпоративних мережах							
Тема 9. Забезпечення безпеки інформації в корпоративних мережах	28	4		6	4		14
Модульний контроль	2						
Разом	30	4		6	4		14
Підготовка та проходження контрольних заходів	60						
Усього	300	36		38	38		112

5. Програма навчальної дисципліни

СЕМЕСТР 4

Змістовий модуль 1. Технології забезпечення безпеки мережевої інфраструктури

Основні питання:

- Побудова захищених мереж відповідно до моделі OSI
- Забезпечення безпеки мережевої інфраструктури
- Контроль доступу користувачів до ІТС
- Виявлення мережевих атак шляхом аналізу трафіку
- Аналіз трафіку комп'ютерних мереж і сценарії атаки типу MITM

Змістовий модуль 2. Захист трафіку за технологією VLAN та тунелювання

Основні питання:

- Загальні відомості щодо побудови VLAN та тунелювання
- Засоби забезпечення захисту трафіку шляхом організації VLAN та тунелювання
- Дослідження організації тунельного з’єднання за протоколами PPTP, L2TP, IPSec, OpenVPN

- Налагодження VPN з'єднання и сервера

Змістовий модуль 3. Визначення вихідних даних щодо створення КСЗІ в ІТС
Основні питання:
- Формування моделі загроз безпеки інформації в ІТС
- Формування моделі порушника безпеки інформації в ІТС
- Модель загроз. Порядок визначення загроз безпеки інформації підприємства
- Модель порушника. Характеристики порушників безпеки інформації.

Змістовий модуль 4. Формування політики безпеки інформації в ІТС
Основні питання:
- Поняття політика безпеки інформації
- Структура критеріїв захищеності інформації та послуг безпеки
- Профіль безпеки інформації в ІТС
- Дослідження побудови функціонального профілю захищеності
- Дослідження побудови функціональних послуг захисту

Змістовий модуль 5. Системи запобігання витоку інформації
Основні питання:
- Характеристика систем запобігання витоку інформації
- Загальна характеристика і принципи функціонування DLP -системи
- Налаштування параметрів функціонування системи запобігання витоку інформації
- Порядок моніторингу просочувань конфіденційної інформації

Змістовий модуль 6. Системи запобігання витоку інформації
Основні питання:
- Загальна характеристика систем виявлення вторгнень
- Політики виявлення вторгнень
- Реалізація оперативного контролю за діями користувачів
- Порядок моніторингу просочувань конфіденційної інформації

СЕМЕСТР 5

Змістовий модуль 7. Управління доступом в мережі. Захист електронної пошти
Основні питання:
- Управління доступом в мережі для базових операційних систем
- Аналіз загроз у відкритих мережах
- Оцінка стійкості парольних систем аутентифікації
- Механізми захисту електронної пошти
- Використання програмного пакету Gpg4win для шифрування і цифрового підпису повідомлень
- Налаштування PGP для шифрування і цифрового підпису повідомлень

Змістовий модуль 8. Забезпечення безпеки інформації в корпоративних мережах
Основні питання:
- Основи безпеки інформаційних сервісів в корпоративних мережах
- Налаштування FTP-серверів
- Забезпечення безпеки в інформації в корпоративних мережах за допомогою брандмауерів
- Налаштування брандмауера в Windows. Налаштування брандмауера Windows за допомогою групової політики

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, залік.
- *Комп'ютерного контролю:* програми - емулятори.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю у 4 семестрі

Вид діяльності студента	Максимальна кількість балів за одиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4		Модуль 5		Модуль 6	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	3	3	2	2	2	2	3	3	2	2	2	2
Відвідування практичних занять	1	2	2	2	2	3	3	2	2	2	2	3	3
Відвідування лабораторних занять	1	2	2	3	3	2	2	2	2	3	3	2	2
Робота на практичному занятті	10	2	20	2	20	3	30	2	20	2	20	3	30
Лабораторна робота	10	2	20	3	30	2	20	2	20	3	30	2	20
Виконання завдань для самостійної роботи	5	3	15	2	10	2	10	3	15	2	10	2	10
Виконання модульної роботи	25	1	25	1	25	1	25	1	25	1	25	1	25
Разом		-	87		92		92		87		92		92
Максимальна кількість балів: 542													
Розрахунок коефіцієнта: 542/100=5,42													

Розрахунок рейтингових балів за видами поточного (модульного) контролю у 5 семестрі

Вид діяльності студента	Максимальна кількість балів за одиницю	Модуль 7		Модуль 8	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	2	2	2	2
Відвідування практичних занять	1	2	2	2	3
Відвідування лабораторних занять	1	3	3	2	2
Робота на практичному занятті	10	2	20	3	30
Лабораторна робота	10	3	30	2	20
Виконання завдань для самостійної роботи	5	2	10	2	10
Виконання модульної роботи	25	1	25	1	25
Разом		-	92		92
Максимальна кількість балів: 184					
Розрахунок коефіцієнта: 184/60=3,07					

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Технології забезпечення безпеки мережевої інфраструктури		14	15
1	Тема 1. Технології забезпечення безпеки мережевої інфраструктури.	14	15

№ з/п	Назва теми	Кількість годин	Бали
	Лекція 1 Побудова захищених мереж відповідно до моделі OSI: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	4	5
	Лекція 2 Забезпечення безпеки мережевої інфраструктури: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	5	5
	Лекція 3. Контроль доступу користувачів до ІТС: опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	5	5
Змістовий модуль 2. Адміністрування захищених ІТ систем і мереж.		14	10
2	Тема 2. Захист трафіку за технологією VLAN та тунелювання.	14	10
	Лекція 1. Загальні відомості щодо побудови VLAN та тунелювання: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	7	5
	Лекція 2 Засоби забезпечення захисту трафіку шляхом організації VLAN та тунелювання: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	7	5
Змістовий модуль 3. Визначення вихідних даних щодо створення КСЗІ в ІТС.		14	10
3	Тема 3. Визначення вихідних даних щодо створення КСЗІ в ІТС.	14	10
	Лекція 1. Формування моделі загроз безпеки інформації в ІТС: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	7	5
	Лекція 2. Формування моделі порушника безпеки інформації в ІТС: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	7	5
Змістовий модуль 4. Моніторинг захищених ІТ систем і мереж. Основи застосування DLP-систем		14	15
4	Тема 4. Формування політики безпеки інформації в ІТС.	14	15
	Лекція 1. Поняття політика безпеки інформації: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	4	5
	Лекція 2. Структура критеріїв захищеності інформації та послуг безпеки: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	5	5
	Лекція 3. Профіль безпеки інформації в ІТС: опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	5	5
Змістовий модуль 5. Аудит захищених ІТ систем і мереж.		14	10
5	Тема 5. Системи запобігання витоку інформації.	14	10
	Лекція 1. Характеристика систем запобігання витоку інформації: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	7	5
	Лекція 2. Загальна характеристика і принципи функціонування DLP - системи: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	7	5
Змістовий модуль 6. Системи виявлення запобігання вторгненням.		14	10
6	Тема 6. Аудит захищених ІТ систем і мереж та системи безпеки.	14	10

№ з/п	Назва теми	Кількість годин	Бали
	Лекція 1. Загальна характеристика систем виявлення вторгнень: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	7	5
	Лекція 2. Політики виявлення вторгнень: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	7	5
Змістовий модуль 7. Управління доступом в мережі. Захист електронної пошти.		14	10
7	Тема 7. Управління доступом в мережі. Захист електронної пошти.	8	5
	Лекція 1. Управління доступом в мережі для базових операційних систем: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	8	5
	Тема 8. Механізми захисту електронної пошти.	6	5
	Лекція 1. Механізми захисту електронної пошти: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	6	5
Змістовий модуль 8. Забезпечення безпеки інформації в корпоративних мережах.		14	10
6	Тема 9. **Забезпечення безпеки інформації в корпоративних мережах**.	14	10
	Лекція 1. Основи безпеки інформаційних сервісів в корпоративних мережах: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	7	5
	Лекція 2. Забезпечення безпеки в інформації в корпоративних мережах за допомогою брандмауерів: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	7	5
	Разом	112	90

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв’язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – модульна контрольна робота, що складається 3 комплексних запитань.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання у 4-му семестрі здійснюється у формі заліку, умовою отримання якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Підсумкове оцінювання у 5-му семестрі здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – комбінована. Іспит оцінюється у 40 балів за розподілом: 20 балів – комплексний тест з дисципліни; 20 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями з побудови інформаційних мереж та управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

Оцінювання практичного завдання відбувається в межах від 0 до 20 балів, згідно критеріїв оцінювання, й здійснюється з урахуванням: рівнів сформованості аналітико-синтетичних, творчих та методичних умінь необхідних для побудови захищених інформаційних та інформаційно-телекомунікаційних (автоматизованих) систем.

Бали за виконання тесту та бали за виконання практичного завдання додаються. Оцінювання результатів засвоєння теоретичних знань та оцінювання сформованості практичних навичок володіння цифровими технологіями студентами, продемонстровані на екзамені, представлене у таблиці.

Підсумкова кількість балів (max – 40)	Оцінка за 4-бальною шкалою
1 – 23	«незадовільно»
24 – 29	«задовільно»
30 – 35	«добре»
36 – 40	«відмінно»

Орієнтовний перелік питань для семестрового контролю

1. Фактори (технологічні та науково-технічні), що впливають на необхідність захисту інформації
2. Види інформації відповідно Закону України "Про інформацію".
3. Властивості інформації.
4. Характерні особливості інформації для захищених ІТС
5. Загрози безпеці інформації та інформаційних ресурсів.
6. Джерела загроз безпеці інформації та інформаційних ресурсів.
7. Характеристика загальних принципів захисту інформації.
8. Заходи, що виконує система захисту інформації.
9. Принципи побудови типової система захисту інформації
10. Характеристика канального шифрування.
11. Характеристика абонентського шифрування.
12. Протокол міжмережного захисту Kerberos
13. Класифікація віддалених атак.
14. Середовища, в яких знаходиться інформації та групи факторів, що впливають на забезпечення інформаційної безпеки.
15. Зміст обстеження обчислювальної системи ІТС.
16. Зміст обстеження фізичного середовища.
17. Зміст обстеження середовища користувачів.
18. Зміст обстеження інформаційного середовища та технології обробки інформації
19. Зміст Моделі порушника.
20. Навмисні загрози інформації
21. Ресурси, що підлягають захисту
22. Зміст робіт із захисту інформації від несанкціонованого доступу.
23. Документи із захисту інформації від витоку її технічними каналами
24. Випадкові загрози інформації та загрози об'єктивного характеру
25. Типи загроз інформації

26. Методи оцінки можливих загроз інформації
27. Класифікація загроз інформації за впливом (характером)
28. Класифікація загроз інформації за наслідками
29. Зміст загроз конфіденційності, цілісності, доступності, спостереженості.
30. Зміст обстеження обчислювальної системи ІТС.
31. Зміст обстеження фізичного середовища.
32. Зміст обстеження середовища користувачів.
33. Зміст обстеження інформаційного середовища та технології обробки інформації
34. Зміст Моделі порушника.
35. Напрями забезпечення захисту інформації в інформаційних і комунікаційних системах
36. Найбільш поширені сценарії несанкціонованого доступу до інформації.
37. Загальні принципи захисту інформації.
38. Елементи системи інформаційної безпеки щодо захисту інформації.
39. Завдання фахівців з планування комплексних систем інформаційної безпеки.
40. Середовища виникнення джерел загроз інформації.
41. Способи несанкціонованого доступу до інформації.
42. Методи реалізації несанкціонованого доступу до інформації
43. Метод реалізації несанкціонованого доступу до інформації Використання комп'ютерного вірусу
44. Метод реалізації несанкціонованого доступу до інформації Використання програми-імітатора
45. Структура типової системи захисту інформації.
46. Завдання підсистеми захисту локальних робочих місць.
47. Завдання підсистем захисту локальної обчислювальної мережі та межмережевої взаємодії.
48. Завдання підсистеми контролю і реєстрації.
49. Характеристика загальних принципів захисту інформації.
50. Заходи, що виконує система захисту інформації.
51. Принципи побудови типової система захисту інформації
52. Фактори внутрішнього і зовнішнього середовища, що впливають на необхідність захисту інформації.
53. Групи факторів, що впливають на захист інформації в інформаційних і комунікаційних системах.
54. Фактори, що впливають на захист інформації, які пов’язані з діяльністю людини.
55. Технологічні фактори та фактори рівня досягнень науково-технічного прогресу, що впливають на захист інформації.
56. Напрями забезпечення захисту інформації в інформаційних і комунікаційних системах.
57. Вимоги до стратегічних рішень.
58. Характеристика та зміст стратегій захисту інформації.
59. Задачі щодо забезпечення безпеки інформаційних технологій.
60. Принципи захисту інформації.
61. Основні принципи побудови системи забезпечення безпеки інформації.
62. Множина загроз інформації в інформаційно-комунікаційних системах (загрози порушення конфіденційності).
63. Множина загроз інформації в інформаційно-комунікаційних системах (загрози порушення цілісності).
64. Множина загроз інформації в інформаційно-комунікаційних системах (загрози порушення доступності чи відмовлення в обслуговуванні).
65. Множина загроз інформації в інформаційно-комунікаційних системах (загрози порушення спостережності чи керованості).
66. Джерела загроз безпеці інформації.

67. Класифікація середовищ виникнення джерел загроз.
68.
69. Підмножини потоків інформаційно-телекомунікаційній системи, що пов’язані з несанкціонованим доступом.
70. Структура множини об’єктів доступу в інформаційно-телекомунікаційній системі.
71. Реалізація послідовності доступів до об’єктів в інформаційно-телекомунікаційній системі.
72. Правила реалізації доступу до об’єктів в інформаційно-телекомунікаційній системі.
73. Зміст множини асоційованих об’єктів.
74. Характеристики множини асоційованих об’єктів.
75. Порядок налаштування локальної політики безпеки.
76. Основні правила брандмауера в Windows 10.
77. Порядок настроювання політик блокування облікових записів користувачів.
78. Основні функції брандмауера в Windows 10.
79. Порядок настроювання безпеки доступу користувачів і груп до файлів.
80. Прядок налаштування клієнта OpenVPN на Windows.
81. Основні операції сервера з перевірки користувача і визначенню дозволеного рівня доступу.
82. Порядок налаштування VPN з’єднання и сервера на Windows 10, 8, 7.
83. Рівні дозволів NTFS.
84. Форми використання NAT.
85. Рівні дозволів сервера.
86. Особливості побудови локальної мережі при підключенні до мережі Інтернет.
87. Захист електронної пошти. Система S/MIME.
88. Особливості побудови мережі з proxy-сервером.
89. Функції системи S/MIME.
90. Особливості побудови мережі з другим Firewall’ом (брандмауером).
91. Порядок використання S/MIME для автентифікації і забезпечення конфіденційності електронної пошти.
92. Особливості побудови мережі з демілітаризованою зоною.
93. Захист електронної пошти. Система PGP.
94. Особливості побудови мережі з використанням для заміни внутрішніх адрес пулу виділених адрес.
95. Коротка характеристика функцій системи PGP.
96. Особливості побудови мережі з використанням групи внутрішніх адрес до однієї зовнішньої.
97. Порядок передачі та отримання повідомлення в системі PGP.
98. Особливості побудови мережі на основі листів доступу.
99. Схема скріплення довіри підпису і відповідності ключа в системі PGP.
100. Механізми реалізації типових віддалених атак.
101. Особливості використання ПО Shadow Security Scanner.
102. Розподіл функцій безпеки за рівнями еталонної моделі OSI.
103. Засоби для віддаленого друку, надання віддаленого доступу до файлів і дисків.
104. Порядок відправки і отримання зашифрованих повідомлень PGP в Windows за допомогою програмного пакету Gpg4win.
105. Короткий список найбільш поширених сервісів в корпоративних мережах.
106. Порядок відправки і отримання зашифрованих повідомлень PGP в Windows за допомогою програмного пакету Gpg4win.
107. Короткий список найбільш поширених сервісів в корпоративних мережах.
108. Порядок використання PGP з декількома обліковими записами електронної пошти.
109. Віддалений доступ до інформаційних сервісів в корпоративних мережах.
110. Характеристики критеріїв захищеності інформації та послуг, що забезпечують захист від загроз.

111. Послуги, що забезпечують захист від загроз за критерієм доступності.
112. Послуги, що забезпечують захист від загроз за критерієм спостереженості.
113. Зміст загроз конфіденційності, цілісності, доступності, спостереженості.
114. Основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз.
115. Обстеження обчислювальної системи ІТС.
116. Обстеження середовища користувачів.
117. Обстеження інформаційного середовищ.
118. Обстеження технології обробки інформації.
119. Обстеження фізичного середовища.
120. Зміст моделі порушника.
121. Класифікація моделей порушника за ступенем деталізації.
122. Структура змістовної моделі порушника.
123. Сценарні моделі порушника.
124. Порядок розробки політики безпеки.
125. Захист електронної пошти. Система PGP.
126. Схема використання S/MIME для автентифікації і забезпечення конфіденційності електронної пошти.
127. Захист електронної пошти. Система S/MIME.
128. Механізми захисту електронної пошти.
129. Управління доступом в мережевій технології «клієнт-сервер».
130. Налашування локальної політики безпеки.
131. Побудова мережі з proxy-сервером.
132. Побудова мережі з демілітаризованою зоною.
133. Побудова мережі з використанням для заміни внутрішніх адрес пулу виділених адрес.
134. Застосування технології NAT для захисту мережі.
135. Проблеми безпеки інформаційних сервісів в корпоративних мережах.
136. Розподіл функцій безпеки за рівнями еталонної моделі OSI.
137. Засоби для надання віддаленого доступу до файлів і дисків.
138. Режими віддаленого доступу до інформаційних сервісів.

Шкала відповідності оцінок

Рейтингова оцінка	Сума балів за всі види навчальної діяльності	Значення оцінки
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов'язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 300 год., лекції – 36 год., практичні заняття – 38 год., лабораторні роботи – 38 год., модульний контроль –16 год., самостійна робота –112 год.

<table>
<tr><td>Модулі (назви, бали)</td><td colspan="3">Змістовий модуль 1 Технології забезпечення безпеки мережевої інфраструктури (87 балів)</td><td colspan="2">Змістовий модуль 2. Захист трафіку за технологією VLAN та тунелювання (92 бали)</td><td colspan="2">Змістовий модуль 3. Визначення вихідних даних щодо створення КСЗІ в ІТС (92 бали)</td></tr>
<tr><td>Лекції (теми, бали)</td><td>Побудова захищених мереж відповідно до моделі OSI (1 бал)</td><td>Забезпечення безпеки мережевої інфраструктури (1 бал)</td><td>Контроль доступу користувачів до ІТС (1 бал)</td><td>Загальні відомості щодо побудови VLAN та тунелювання (1 бал)</td><td>Засоби забезпечення захисту трафіку шляхом організації VLAN та тунелювання (1 бал)</td><td>Формування моделі загроз безпеки інформації в ІТС (1 бал)</td><td>Формування моделі порушника безпеки інформації в ІТС (1 бал)</td></tr>
<tr><td>Практичні, семінарські заняття (теми, бали)</td><td></td><td colspan="2">Аналіз трафіку комп'ютерних мереж і сценарії атаки типу MITM (Man - in - the - Middle) (22 бали)</td><td></td><td>Дослідження організації тунельного з’єднання за протоколами PPTP, L2TP, IPSec, OpenVPN. (22 бали)</td><td></td><td>Порядок формування моделі порушника безпеки інформації в ІТС (33 бали)</td></tr>
<tr><td>Лабораторні заняття (теми, бали)</td><td colspan="2">Виявлення мережевих атак шляхом аналізу трафіка (22 бали)</td><td></td><td>Налагодження VPN з’єднання и сервера. (33 бали)</td><td></td><td>Порядок формування моделі загроз безпеки інформації в ІТС. (22 бали)</td><td></td></tr>
<tr><td>Самостійна робота</td><td colspan="3">Самостійна робота (15 балів)</td><td colspan="2">Самостійна робота (10 балів)</td><td colspan="2">Самостійна робота (10 балів)</td></tr>
<tr><td>Поточний контроль (вид, бали)</td><td colspan="3">Модульна контрольна робота 1 (25 балів)</td><td colspan="2">Модульна контрольна робота 2 (25 балів)</td><td colspan="2">Модульна контрольна робота 3 (25 балів)</td></tr>
</table>

Модулі (назви, бали)	**Змістовий модуль 4. Формування політики безпеки інформації в ІТС (87 балів)**			**Змістовий модуль 5. Системи запобігання витоку інформації (92 бали)**		**Змістовий модуль 6. Системи виявлення запобігання вторгненням (92 бали)**	
Лекції (теми, бали)	Поняття політика безпеки інформації (1 бал)	Структура критеріїв захищеності інформації та послуг безпеки (1 бал)	Профіль безпеки інформації в ІТС (1 бал)	Характеристика систем запобігання витоку інформації (1 бал)	Загальна характеристика і принципи функціонування DLP - системи (1 бал)	Загальна характеристика систем виявлення вторгнень (1 бал)	Політики виявлення вторгнень (1 бал)
Практичні, семінарські заняття (теми, бали)		Дослідження побудови функціонального профілю захищеності (22 бали)			Порядок моніторингу просочувань конфіденційної інформації (22 бали)		Порядок моніторингу просочувань конфіденційної інформації (33 бали)
Лабораторні заняття (теми, бали)	Дослідження побудови функціональних послуг захисту. (22 бали)			Налаштування параметрів функціонування системи запобігання витоку інформації (33 бали)		Реалізація оперативного контролю за діями користувачів (22 бали)	
Самостійна робота	Самостійна робота (15 балів)			Самостійна робота (10 балів)		Самостійна робота (10 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 4 (25 балів)			Модульна контрольна робота 5 (25 балів)		Модульна контрольна робота 6 (25 балів)	
Підсумковий контроль (вид, бали)	Залік						

Модулі (назви, бали)	**Змістовий модуль 7 Управління доступом в мережі. Захист електронної пошти (92 бали)**		**Змістовий модуль 8 Забезпечення безпеки інформації в корпоративних мережах (92 бали)**	
Лекції (теми, бали)	Управління доступом в мережі для базових операційних систем (1 бал)	Механізми захисту електронної пошти (1 бал)	Основи безпеки інформаційних сервісів в корпоративних мережах (1 бал)	Забезпечення безпеки в інформації в корпоративних мережах за допомогою брандмауерів (1 бал)
Практичні, семінарські заняття (теми, бали)	Оцінка стійкості парольних систем аутентифікації (11 балів)	Налаштування PGP для шифрування і цифрового підпису повідомлень (11 балів)	Налаштування FTP-серверів (11 балів)	Налаштування брандмауера в Windows (22 бали)
Лабораторні заняття (теми, бали)	Аналіз загроз у відкритих мережах (11 балів)	Використання програмного пакету Gpg4win для шифрування і цифрового підпису повідомлень (22 бали)		Налаштування брандмауера Windows за допомогою групової політики (22 бали)
Самостійна робота	Самостійна робота (10 балів)		Самостійна робота (10 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота (25 балів)		Модульна контрольна робота (25 балів)	
Підсумковий контроль (вид, бали)	Екзамен (40 балів)			

8. Рекомендовані джерела

Основна (базова):

1. Богуш В.М., Кудін А.М. Інформаційна безпека від А до Я: 3000 термінів і понять. - К.: МОУ, 1999. - 456 с.
2. Богуш В.М., Юдін О.К. Основи інформаційної безпеки держави. – К.: “МК-Прес”, 2005 – 432 с.
3. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
4. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В. Толюпа, В.В. Семко, Л.В. Бурячок, П.М. Складанний Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178 с
5. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М. Технології забезпечення безпеки мережевої інфраструктури: підручник. К.: КУБГ, 2019. 225 с.
6. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.
7. ДСТУ 2462--94. Сертифікація. Основні поняття. Терміни та визначення.- К.: Держстандарт України, 1994. - 24 с.
8. ДСТУ 2874--94. Системи обробки інформації. Бази даних. Терміни та визначення.
9. ДСТУ 2938--94. Системи оброблення інформації. Основні поняття. Терміни та визначення.
10. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
11. Комп’ютерні мережі: навч. посіб. для технічних спец. вищих навч. закл. Кн. 2. - Львів: Магнолія 2006, 2014. - 327 с.

Додаткова

1. Scott Mueller. Upgrading and Repairing Networks, Third Edition. Que, 2002.
2. Panoc C. Lekkas. Network Processors. The McGraw-Hill Companies, 2003.
3. International Standard ISO/IEC 17799. Information technology - Code of practice for information security management. First edition 2000-12-01.
4. International Standard ISO 7498-2: 1989 Information processing systems. - Open Systems Interconnection. - Basic Reference Model. - Part 2: Security Architecture. - First edition. -15.02.1989. - 32 р.ДСТУ 2226--93. Автоматизовані системи. Терміни та визначення.

9. Додаткові ресурси

1. History of LAN Switching. [електронний ресурс] http://www.myipaddressinfo.com
2. Evolution: 20 years of switching fabric. Ori Aruj, Dune Networks [електронний ресурс] http://www.commsdesign.com
3. On-chip Global Interconnects for Networking ASICs [електронний ресурс] http://www.lsi.com
4. Andreas D. Bovopoulos and Micha Zeiger. Shared-Memory Fabrics Meet 10-Gbit Backplane Demands. TeraChip, Inc. [електронний ресурс] http://www.commsdesign.com
5. Matching Output Queueing with a Combined Input Output Queued Switch [електронний ресурс] http://www-rcf.usc.edu
6. An improved algorithm for CIOQ switches. Yossi Azar, Ybssi Richter. [електронний ресурс] http://portal.acm.org
7. Institute of Electrical and Electronics Engineers) [електронний ресурс] http://www.ieee.org