Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра безпеки інформаційних систем і технологій

“ЗАТВЕРДЖУЮ”

Проректор з науково – педагогічної роботи

Олександр ГОЛОВКО

“____”_____2022 р.

Робоча програма навчальної дисципліни

«Управління інформаційною безпекою»

рівень вищої освіти перший (бакалаврський)

галузь знань 012 - Інформаційні технології

спеціальність 125- Кібербезпека

освітня програма Кібербезпека

спеціалізація

вид дисциплін обов’язкова

факультет комп’ютерних наук

2022 / 2023

2

Програму обговорено та рекомендовано до затвердження вченою радою факультету комп'ютерних наук "28 " червня 2022 року, протокол №10

РОЗРОБНИКИ ПРОГРАМИ:
Малахов Сергій Віталійович, кандідат технічних наук, старшій науковий співробитник, доцент кафедри безпеки інформаційних систем і технологій

Програму схвалено на засіданні кафедри безпеки інформаційних систем і технологій
Протокол від " 23 " червня 2022 року № 10

Завідувач кафедри безпеки інформаційних систем і технологій

Сергій Рассомахін

Гарант освітньої (професійної/наукової) програми

(керівник проєктної групи) Рассомахін Сергій Геннадійович

Сергій Рассомахін

Програму погоджено методичною комісією факультету комп'ютерних наук

Протокол від "24 "червня 2022 року №9

Голова методичної комісії факультету комп'ютерних наук

Анатолій Бердников

ВСТУП

Програма навчальної дисципліни «Управління інформаційною безпекою» (далі- УІБ) складена відповідно до освітньої програми підготовки першого (бакалаврського) рівня за спеціальністю 125 «Кібербезпека».

1. Опис навчальної дисципліни

1.1. Мета навчальної дисципліни

Дисципліна має на меті: отримання студентами необхідних знань щодо принципів створення комплексних систем захисту інформації (КСЗІ) в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах (далі – ІТС), здійснення комплексу заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують обробку інформації в ІТС згідно з вимогами, встановленими нормативно – правовими актами та нормативними документами у сфері захисту інформації, а також принципів проведення експертизи КСЗІ, отримання студентами необхідних базових знань з організації та проведення аудиту інформаційної безпеки (ІБ), управління і оцінки ризиків ІБ в інформаційно-телекомунікаційних системах різного призначення.

.

1.2. Основні завдання дисципліни:

Основними завданнями вивчення дисципліни є: формування у студентів певних знань та вмінь з теорії та практики побудови та аналізу систем управління інформаційною безпекою в ІТС організацій, установ, підприємств у відповідності із вітчизняною і міжнародною нормативно-правовою базою.

1.3. Кількість кредитів – 4.

1.4. Загальна кількість годин – 120.

1.5. Характеристика навчальної дисципліни	
Нормативна	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
4-й	-
Семестр	
8-й	-
Лекції	
24 год.	-
Практичні, семінарські заняття	
24 год.	-
Лабораторні заняття	
-	-
Самостійна робота	
72 год.	-
Індивідуальні завдання	
Індивідуальні завдання не застосовуються	

1.6. Заплановані результати навчання:

У результаті вивчення даного курсу студент повинен:

знати:

- національну та міжнародну нормативно правову базу, науково-методичні та технічні принципи організації, впровадження та застосування систем управління захистом інформації в ІТС;
- принципи створення КСЗІ в ІТС;
- організацію та порядок проведення робіт з проектування, впровадження та супроводу комплексних систем захисту інформації в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах;
- організацію та порядок проведення робіт з державної експертизи КСЗІ та засобів захисту інформації;
- вимоги міжнародних стандартів та вітчизняних нормативних документів в сфері захисту інформації щодо управління захистом інформації в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах.
- вимоги міжнародних стандартів в галузі управління інформаційною безпекою;
- методи, методики, програмні засоби оцінки ризиків інформаційної безпеки в ІТС підприємств, установ, організацій.

уміти:

- здійснювати заходи щодо проектування, впровадження та супроводу, систем управління захистом інформації в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах;
- застосовувати вимоги міжнародних стандартів та вітчизняних нормативних документів в сфері захисту інформації при проведенні державної експертизи КСЗІ та засобів захисту інформації, аудиту інформаційних систем та інформаційної безпеки, сертифікації систем управління інформаційно безпекою на відповідність вимогам відповідних міжнародних стандартів
- складати моделі загроз безпеки інформації та моделі потенційних порушників;

бути ознайомленими з:

- основними положеннями організації та функціонування захищених інформаційних систем (ІС), телекомунікаційних систем (ТС) та інформаційно - телекомунікаційних систем різного призначення;
- міжнародними стандартами та нормативними документи Держспецзв'язку України щодо створення системи управління інформаційною безпекою з метою захисту державних інформаційних ресурсів, інформації з обмеженим доступом, в тому числі персональних даних.

2. Тематичний план навчальної дисципліни

Розділ 1. Концепція побудови захищеної інформаційно-телекомунікаційної системи (ІТС)**.**

Тема 1. Безпека корпоративних мереж. Проблематика безпеки IP мереж. Модель протидії загрозам безпеки. Побудова підсистеми інформаційної безпеки. Шляхи рішення проблем захисту інформації.

Тема 2. Концепція захищеної інформаційно-телекомунікаційної системи. Принципи створення захищеної інформаційно-телекомунікаційної системи. Концептуальна модель інформаційної безпеки організації. Структура концепції. Мета та завдання забезпечення безпеки інформації в ІТС організації.

Тема 3. Стратегія, основні напрямки та методи забезпечення безпеки інформації. Організаційна структура системи забезпечення безпеки інформації.

Розділ 2. Методологія управління інформаційною безпекою.
Тема 4. Концепція управління інформаційною безпекою**.** Принципи управління захистом інформації в ІТС. Задачі управління захистом інформації в ІТС. Глобальна і локальні політики управління захистом інформації в ІТС.
Тема 5. Міжнародні та вітчизняні стандарти в галузі управління, оцінки та аудиту інформаційної безпеки. Планування аудиту інформаційної безпеки організації. Управління аудитом інформаційної безпеки. Процесна модель управління інформаційною безпекою.
Тема 6. Технології аудиту інформаційної безпеки. Практичні шаги аудиту інформаційної безпеки. Задачі, що вирішуються при проведенні аудиту. Принципи аналізу і управління інформаційними ризиками. Методологія оцінки ризиків інформаційної безпеки. Перспективні методи оцінки ризиків інформаційної безпеки. Оцінка інформаційних ризиків з використання методів системного аналізу.
Тема 7. Технологія виявлення атак та аналізу захищеності ІТС. Засоби аналізу захищеності. Архітектура систем виявлення атак. Класифікація систем виявлення атак.
Індивідуальне дослідне завдання.

3. Структура навчальної дисципліни

Назви розділів	Кількість годин						
	денна форма						
	усього	у тому числі					
		л	п	лаб.	інд.	с. р.	
1	2	3	4	5	6	7	
Розділ 1. Концепція побудови захищеної інформаційно-телекомунікаційної системи (ІТС)**.**							
Тема 1. Безпека корпоративних мереж.	14	2	2			10	
Тема 2. Концепція захищеної інформаційно-телекомунікаційної системи.	18	4	4			10	
Тема 3. Стратегія, основні напрямки та методи забезпечення безпеки інформації.	18	4	4			10	
Разом за розділом 1	50	10	10			30	
Розділ 2. Методологія управління інформаційною безпекою.							
Тема 4. Концепція управління інформаційною безпекою**.**	16	3	3			10	
Тема 5. Міжнародні та вітчизняні стандарти в галузі управління, оцінки та аудиту інформаційної безпеки.	20	4	4			12	
Тема 6. Технології аудиту інформаційної	16	3	3			10	

безпеки.							
Тема 7. Технологія виявлення атак та аналізу захищеності ІТС.	18	4	4			10	
Разом за розділом 2	70	14	14			42	
Усього годин	90	24	24			72	

4 Теми семінарських (практичних) занять

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	Модель загроз. Модель протидії загрозам безпеки. Шляхи рішення проблем захисту інформації.	4
2	Концептуальна модель інформаційної безпеки організації. Побудова підсистеми інформаційної безпеки.	4
3	Організаційна структура системи забезпечення безпеки інформації. Служба захисту інформації (СЗІ). Функції, завдання, відповідальність, штатна структура СЗІ.	4
5	Міжнародні та вітчизняні стандарти в галузі управління, оцінки та аудиту інформаційної безпеки. Процесна модель управління інформаційною безпекою.	4
6	Методи оцінки ризиків інформаційної безпеки. Оцінка інформаційних ризиків з використання методів системного аналізу.	4
7	Засоби аналізу захищеності ІТС. Виявлення атак та управління інформаційними ризиками.	4
	Разом	24

5. Завдання для самостійної роботи

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	Підготовка до практичних занять та виконання домашніх завдань	20
2	Підготовка до лекційних занять та виконання завдань	20
3	Підготовка до тестування залишкових знань	20
4	Підготовка до контрольної роботи	12
	Разом (год)	72

6. Індивідуальні завдання

Індивідуальні завдання не застосовуються.

7. Методи навчання

Як правило лекційні та практичні заняття проводяться аудиторне. В умовах дії карантину заняття проводяться відповідно до Наказу ректора Харківського національного університету імені В.Н. Каразіна (аудиторне або дистанційно за допомогою платформ Google Meet або Zoom)

8. Методи контролю

Контроль засвоєння студентами навчального матеріалу на лекційному зайнятті здійснюється шляхом концентрації уваги студентів постановкою питань за раніше вивченим матеріалом, пов'язаним з тематикою лекції.

Присутність студента на зайнятті оцінюється в 0,5 балу. Максимальна кількість балів за присутність студента на зайнятті складає 12 балів.

На практичному зайнятті контроль знань студентів робиться методом проведення експрес-опитувань (письмово). Рівень знань, продемонстрований студентами на кожному експрес-опитуванні оцінюється 2 балами.

Максимальна кількість балів за результатами контролю поточної успішності складає 60 балів.

Підсумковий контроль здійснюється шляхом проведення іспиту.

Екзаменаційний квиток включає два теоретичних і одне практичне питання. Теоретичні питання оцінюються в 10 балів, практичний - в 15, кожен.

Максимальна кількість балів за результатами іспиту складає 40 балів.

Максимальна кількість балів за результатами вивчення дисципліні складає 100 балів.

9. Схема нарахування балів

Бали за поточний контроль знань по розділу 1 протягом семестру (по темах)							Контрольна робота, передбачена навчальним планом	Разом сума балів у семестрі	Іспит	Загальна сума балів
Т1	Т2	Т3	Т4	Т5	Т6	Т7				
4	6	6	6	8	4	6	20	60	40	100

Т1, Т2, Т3, Т4 ... – теми занять.

Рівень знань, продемонстрований студентами, оцінюється таким чином:

- за темою 1(Т1) – 4 бал: 2 заняття; 2експрес-опитування;
- за темою 2(Т2) –6 бали: 4 заняття, 3 експрес-опитування;
- за темою 3(Т3) – 6 бали: 4 заняття, 3 експрес-опитування;
- за темою 4 (Т4) – 6 бали: 3 заняття, 3 експрес-опитування;
- за темою 5 (Т5) – 8бали: 4 заняття, 4 експрес-опитування;
- за темою 6 (Т6) – 4 бала: 3 заняття, 2 експрес-опитування;
- за темою 7 (Т7) – 6 бали: 4 заняття, 3 експрес-опитування;
- за контрольну роботу (Т1 – Т7) – 20 балів;

Критерії оцінювання знань студентів за виконання контрольній роботи

Визначення	Кількість балів
Дані повні відповіді на кожне практичне питання показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки	20
У відповідях на поставлені практичні питання показано знання навчального матеріалу, розуміння суті поставлених питань за наявності незначних помилок зроблені достатньо повні і правильні	18

висновки	
У відповідях на поставлені практичні питання показано достатньо знання навчального матеріалу при наявності суттєвих помилок, зроблені висновки	14
У відповідях показано розуміння суті поставлених питань за наявності принципових помилок при рішенні практичних завдань, відсутні висновки	10
У відповідях показано слабкі знання навчального матеріалу при наявності принципових помилок при рішенні практичних завдань, відсутні висновки	5

Критерії оцінювання екзаменаційних робіт студентів

Визначення	Кількість балів
При відповіді на екзаменаційний квиток теоретичні питання освітлені повністю, завдання вирішене правильно, зроблені висновки	40
При відповіді на екзаменаційний квиток теоретичні питання достатньо освітлені, завдання вирішене правильно з незначними помилками, зроблені висновки	35-39
При відповіді на екзаменаційний квиток теоретичні питання освітлені з помилками, завдання вирішене правильно з незначними помилками. Зроблені неповні висновки	25-34
При відповіді на екзаменаційний квиток теоретичні питання освітлені з суттєвими помилками, завдання вирішене з помилками. Зроблені неповні висновки	15-24
При відповіді на екзаменаційний квиток теоретичні питання освітлені з суттєвими помилками, завдання вирішене частково або не повністю. Висновки неповні або відсутні	1-14

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка
	для чотирирівневої шкали оцінювання (іспит)
90 – 100	відмінно
70-89	добре
50-69	задовільно
1-49	незадовільно

10. Рекомендована література

Базова література

1. Замула О.А., Горбенко Ю.І., Шумов А.І. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації»: Навч. посібник. - Харків: ХНУРЕ, 2010 - 98 с.
2. За редакцією Горбенко І.Д. Горбенко Ю.І. «Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації». . Монографія. Харків. Форт. 2016 , 902с.
3. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Монографія. Харків. Форт. 2010 , 593с.
4. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків. Форт. 2013р. 878с.

Допоміжна література

5. ДСТУ ISO/IEC 27000: 2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT);
6. ДСТУ ISO/IEC 27001: 2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT);
7. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT);
8. ДСТУ ISO/IEC 27005: 2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT);
9. ДСТУ ISO/IEC 27013:2016 Інформаційні технології. Методи захисту. Настанови до комплексної реалізації ISO/IEC 27001 та ISO/IEC 20000-1 (ISO/IEC 27013:2015, IDT);
10. ДСТУ ISO/IEC 27034 - 1:2016 Інформаційні технології. Методи захисту. Безпека прикладних програм.Част.1. Огляд і концепція (ISO/IEC 27034 - 1:2011/Cor.1:2014, IDT);
11. ДСТУ ISO/IEC 27039 - 1: 2016 Інформаційні технології. Методи захисту. Вибирання, розгортання та експлуатація систем виявлення та запобігання вторгнень (ISO/IEC 27039: 2015, IDT);
12. ДСТУ ISO/IEC 27040 - 1: 2016 Інформаційні технології. Методи захисту. Безпека зберігання (ISO/IEC 27040: 2015, IDT);
13. ДСТУ ISO/IEC 27043 - 1: 2016 Інформаційні технології. Методи захисту. Принципи і процеси розслідування інцидентів (ISO/IEC 27043: 2015, IDT);
14. NIST Special Publication 800-37, Revision 2. Risk Management Framework for Information Systems and Organizations, 2018.