Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра безпеки інформаційних систем і технологій

"ЗАТВЕРДЖУЮ"

Проректор з науково-педагогічної роботи

_____ Антон ПАНТЕЛЕЙМОНОВ

_____ 2020 р.

Робоча програма навчальної дисципліни

Основи інформаційної безпеки держави

рівень вищої освіти __перший (бакалаврський)__

галузь знань 12 «Інформаційні технології»

спеціальність 125 – «Кібербезпека»

освітня програма Кібербезпека

спеціалізація

вид дисципліни ___обов`язкова__

факультет комп`ютерних наук

2020 / 2021 навчальний рік

2

Програму рекомендовано до затвердження вченою радою факультету (інституту, центру)

"31" серпня 2020 року, протокол № 12

РОЗРОБНИКИ ПРОГРАМИ: Замула Олександр Андрійович, доктор технічних наук, доцент, професор кафедри безпеки інформаційних систем і технологій.

Програму схвалено на засіданні кафедри безпеки інформаційних систем і технологій

Протокол від "31" серпня 2020 року № 1

Завідувач кафедри безпеки інформаційних систем і технологій

(підпис) Рассомахін С.Г.
(прізвище та ініціали)

Програму погоджено з гарантом освітньої (професійної/наукової) програми (керівником проектної групи) Кібербезпека

назва освітньої програми

Гарант освітньої (професійної/наукової) програми
(керівник проектної групи) Рассомахін Сергій Геннадійович

(підпис) Рассомахін С. Г.
(прізвище та ініціали)

Програму погоджено методичною комісією факультету комп'ютерних наук

Протокол від "31" серпня 2020 року № 1

Голова методичної комісії факультету комп'ютерних наук

Бердніков А. Г.

Додаток до робочої програми навчальної дисципліни «Основи інформаційної безпеки держави».
Дію робочої програми продовжено: на 2021/2022 н. р.

Заступник декана факультету з навчальної роботи

_____ Євгенія КОЛОВАНОВА

« » серпня 2021 р.

Голова методичної комісії факультету комп'ютерних наук

_____ Анатолій БЕРДНІКОВ

« » серпня 2021 р.

Програму погоджено з гарантом освітньої програми 125 «Кібербезпека»
Гарант освітньої програми 125 «Кібербезпека»

_____ Сергій РАССОМАХІН

ВСТУП

Програма навчальної дисципліни «Основи інформаційної безпеки держави» (далі- ОІБД) 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: засвоєння студентами сукупності загроз інформаційної безпеки; загроз кібербезпеки і безпеки інформаційним ресурсам держави;

- отримання студентами необхідних знань з правових основ захисту інформації в Україні, компетенцій державних установ та інститутів щодо захисту інформації;

- формування компетенції втілення в життя положень державної політики в сфері захисту інформаційних ресурсів відомств, установ, організацій та підприємств.

1.2. Основні завдання дисципліни:

Основними завданнями вивчення дисципліни є: сформувати у студентів уявлення про стратегію національної безпеки України; отримання цілісних знань про основні напрями забезпечення національної безпеки держави в інформаційній сфері.

1.3. Кількість кредитів – 3.

1.4. Загальна кількість годин – 90.

1.5. Характеристика навчальної дисципліни	
Нормативна	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
3-й	-
Семестр	
6-й	-
Лекції	
22 год.	-
Практичні, семінарські заняття	
10 год.	-
Лабораторні заняття	
-	-
Самостійна робота	
58 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 заходів захисту державних інформаційних ресурсів, інформації з обмеженим доступом в ІС, ТС;

- моделі порушників та типові загрози безпеці інформаційним ресурсам ІС, ТС, ІТС державних органів, установ, організацій та підприємств ;
- поняття, види, правові ознаки, класифікацію інформації;
- основи чинного законодавства держави в сфері інформаційної безпеки;
- особливості захисту різних видів інформації з обмеженим доступом (державної таємниці, банківської таємниці тощо).
- проблеми, стан та перспективи створення та застосування заходів захисту державних інформаційних ресурсів, інформації з обмеженим доступом в ІС, ТС, ІТС.

уміти:

- складати моделі загроз безпеці інформації, визначати задачі захисту та розробляти тактико-технічні вимоги до криптосистем та крипто протоколів, включаючи моделі загроз відносно користувачів хмарних сервісів;
- розробляти технічні та часткові технічні завдання на криптосистеми та засоби КЗІ при їх побудові;
- застосовувати отримані знання при експертизі, тематичних дослідженнях та сертифікаційних випробовуваннях криптосистем та засобів КЗІ, в тому числі в пост квантовий період;
- обґрунтувати та проектувати стандартні криптографічні системи, засоби, криптографічні примітиви та протоколи захисту інформації та інформаційних ресурсів в ІТС, включаючи хмарні сервіси;
- здійснювати загальну оцінку якості захисту інформації та правомірність застосування криптосистем систем та засобів КЗІ в ІТС;
- обґрунтовувати вибір архітектури ІВК (системи ЕЦП) з урахуванням завдань, що вирішується на міжнародному рівні та держави, відомства, державних установ, приватних організацій, суспільних організацій;
- виконувати та аналізувати обов’язки посадових осіб служб інформаційної безпеки захищених ІТС(ІС) та центрів сертифікації ключів(ЦСК) згідно діючих регламентів чи діючих політик безпеки.
- моделювати та досліджувати на ПЕОМ та безпосередньо з використанням засобів КЗІ процеси криптографічного захисту інформації та інформаційних ресурсів, криптографічних перетворень, криптографічного аналізу, управління ключами та криптографічні протоколи в ІТС та ІВК, в тому числі користувачам хмарних сервісів.

2. Тематичний план навчальної дисципліни

Розділ 1. Законодавство України в інформаційній сфері та у сфері інформаційної безпеки.

Тема 1. Стратегія національної безпеки України. Актуальні загрози національній безпеці. Місце та роль захисту інформації в системі національної безпеки України. Національна безпека України та її складові частини. Державна політика у сфері інформаційної безпеки. Поняття і зміст інформаційної безпеки України. Загрози інформаційної безпеки.

Тема 2. Загрози кібербезпеці і безпеці інформаційних ресурсів. Принципи забезпечення безпеки інформації в інформаційно – телекомунікаційних системах. Моделі загроз інформаційної безпеки. Мета та задачі захисту інформації в інформаційно – телекомунікаційних системах. Міжнародні стандарти та нормативні документи України в галузі захисту інформації. Розробка Концепції забезпечення інформаційної безпеки

організації. Розробка корпоративної політики забезпечення інформаційної безпеки організації.

Тема 3. Правовий режим захисту державної таємниці. Проблемні питання у сфері захисту інформаційних ресурсів, що віднесені до державної таємниці, та шляхи їх вирішення. Загальні питання доступу до інформації та відповідальність за порушення законодавства про інформацію. Державна таємниця та система її охорони. Віднесення інформації до державної таємниці. Засекречування та розсекречування матеріальних носіїв інформації. Режимно-секретні органи. Допуск громадян до державної таємниці. Доступ громадян до державної таємниці. Обов'язки громадянина щодо збереження державної таємниці. Контроль за забезпеченням охорони державної таємниці. Відповідальність за порушення законодавства про державну таємницю.

Розділ 2. Напрями державної політики України в інформаційній сфері**.**

Тема 4. Ліцензійна та сертифікаційна діяльність у галузі захисту інформації. Законодавство України про ліцензування видів господарчої діяльності. Сертифікація засобів технічного захисту інформації. Правова регламентація охоронної діяльності.

Тема 5. Особливості сучасного етапу розвитку інформаційних технологій та їх вплив на безпеку інформації. Правові основи захисту інформації із застосування технічних засобів. Правовий статус інформації. Поняття, правові ознаки та види інформації. Правовий статус інформації як об'єкта цивільних прав. Зміст суб'єктивного права на інформацію. Інформація – як об'єкт захисту. Захист інтелектуальної власності. Злочини у сфері комп'ютерної інформації. Міжнародне законодавство у галузі захисту інформації.

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин					
	денна форма					
	усього	у тому числі				
		л	п	лаб.	інд.	с. р.
1	2	3	4	5	6	7
1. **Розділ 1.** Законодавство України в інформаційній сфері та у сфері інформаційної безпеки.						
Тема 1. Стратегія національної безпеки України. Актуальні загрози національній безпеці.	12	4			-	8
Тема 2. Загрози кібербезпеці і безпеці інформаційних ресурсів. Принципи забезпечення безпеки інформації в інформаційно – телекомунікаційних системах.	16	4	2		-	10
Тема 3. Проблемні питання та їх вирішення у сфері захисту інформаційних ресурсів, що віднесені до державної таємниці.	18	4	4		-	10
Разом за розділом 1	46	12	6		-	28

Розділ 2. Напрями державної політики України в інформаційній сфері**.**						
Тема 4. Ліцензійна та сертифікаційна діяльність у галузі захисту інформації. Сертифікація засобів технічного захисту інформації.	23	6	2		-	15
Тема 5 Правовий статус інформації. Вимоги чинного законодавства щодо забезпечення інформаційної безпеки.	21	4	2		-	15
Разом за розділом 2	44	10	4		-	30
Всього годин	90	22	10		-	58

4. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Загрози кібербезпеці. Модель протидії загрозам безпеки. Шляхи рішення проблем захисту інформації.	2
2	Організація допуску та доступу до державної таємниці. Організаційно-правові заходи щодо збереження державної таємниці.	4
3	Порядок оформлення ліцензії на провадження господарської діяльності в сфері інформаційної безпеки.	2
4	Методи оцінки ризиків інформаційної безпеки. Оцінка інформаційних ризиків з використання методів системного аналізу.	2

5. Завдання для самостійної роботи студентів

№ з/п	Назва теми	Кількість годин
1	Вивчення конспекту лекцій	10
	Підготовка до практичних занять	10
	Вивчення додаткових матеріалів за темою : Стратегія національної безпеки України. Актуальні загрози національній безпеці.	7
2	Вивчення додаткових матеріалів за темою : Загрози кібербезпеці і безпеці інформаційних ресурсів. Принципи забезпечення безпеки інформації в інформаційно – телекомунікаційних системах.	7
3	Вивчення додаткових матеріалів за темою :Проблемні питання та їх вирішення у сфері захисту інформаційних ресурсів, що віднесені до державної таємниці.	8
4	Вивчення додаткових матеріалів за темою : Ліцензійна та сертифікаційна діяльність у галузі захисту інформації. Сертифікація засобів технічного захисту інформації.	8
5	Вивчення додаткових матеріалів за темою : Правовий статус інформації. Вимоги чинного законодавства щодо забезпечення інформаційної безпеки.	8
Разом		58

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 10 балів.

На практичному зайнятті контроль знань студентів робиться методом проведення експрес-опитувань (письмово). Рівень знань, продемонстрований студентами на кожному експрес-опитуванні оцінюється 2.5 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				
5.5	7.5	10	9.5	7.5	20	60	40	100

Т1, Т2, Т3, Т4 ... – теми занять.

Рівень знань, продемонстрований студентами, оцінюється таким чином:

- за темою 1(Т1) – 5.5балів: 2 заняття; 2 експрес-опитування;
- за темою 2(Т2) –7.5 балів:3 заняття, 2 експрес-опитування;
- за темою 3(Т3) – 10 балів:4 заняття, 3 експрес-опитування;
- за темою 4 (Т4) – 9.5балів: 4 заняття, 3експрес-опитування;
- за темою 5 (Т5) – 7.5 балів: 3 заняття, 2 експрес-опитування;
- за контрольну роботу (Т1 – Т11) – 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 висновки	17
У відповідях на поставлені практичні питання показано достатньо знання навчального матеріалу при наявності суттєвих помилок, зроблені висновки	13
У відповідях показано розуміння суті поставлених питань за наявності принципових помилок при рішенні практичних завдань, відсутні висновки	11
У відповідях показано слабкі знання навчального матеріалу при наявності принципових помилок при рішенні практичних завдань, відсутні висновки	8

Критерії оцінювання залікових 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
	залік
90 – 100	зараховано
70-89	зараховано
50-69	зараховано

1-49	не зараховано

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 - 108 с.
2. Замула О.А. Захист держаних секретів. Навчальний посібник. ХНУРЕ – 2004.– 206 с.
3. За редакцією Горбенко І.Д. Горбенко Ю.І. «Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації». Монографія. Харків. Форт. 2016 , 902с.
4. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків. Форт. 2013р., - 878с.

Допоміжна література

5. Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України";
6. Указ Президента України Про рішення Ради національної безпеки і оборони України 2016 року «Про Доктрину інформаційної безпеки України»;
7. Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації».
8. ДСТУ ISO/IEC 10118-1:2003. Інформаційні технології. Методи захисту. Геш-функції. Частина 1. Загальні положення
9. ДСТУ ISO/IEC 10118-3:2005 «Інформаційні технології. Методи захисту. Геш-функції. Частина 3: Спеціалізовані геш - функції».
10. ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування».
11. ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення».