МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное образовательное учреждение высшего образования
"Курский государственный университет"

Кафедра информационной безопасности

УТВЕРЖДЕНО

протокол заседания
Ученого совета от 30.09.2019 г., №2

Рабочая программа дисциплины
Основы кибербезопасности

Направление подготовки: 38.03.01 ЭКОНОМИКА

Профиль подготовки: Финансы и кредит

Квалификация: бакалавр

Форма обучения: очная

Общая трудоемкость 2 ЗЕТ

Виды контроля в семестрах:

зачет(ы) 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	17			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	18	18	18	18
В том числе инт.	8	8	8	8
Итого ауд.	36	36	36	36
Контактная работа	36	36	36	36
Сам. работа	36	36	36	36
Итого	72	72	72	72

Курск 2019

Рабочая программа дисциплины Основы кибербезопасности / сост. ; Курск. гос. ун-т. - Курск, 2019. - с.

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Минобрнауки России от 12.11.2015 г. № 1327 "Об утверждении ФГОС ВО по направлению подготовки 38.03.01 ЭКОНОМИКА (уровень бакалавриата)"

Рабочая программа дисциплины "Основы кибербезопасности" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 38.03.01 ЭКОНОМИКА профиль Финансы и кредит

Составитель(и):

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Сформировать базовый уровень знаний, умений и владения навыками по обеспечению информационной безопасности информационных систем и информационных ресурсов профессиональной деятельности

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	ФТД.В

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПК-1: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Знать:

Базовые понятия и содержание технологий обеспечения основ кибербезопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах ,а так же процессы управления информационной безопасностью защищаемых объектов

Базовый комплекс мер по обеспечению основ информационной безопасности с учетом их правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности, возможных внешних воздействий, вероятных угроз и уровня развития технологий защиты информации и основные требования содержащееся в нормативно- правовом обеспечении оборота сведений составляющих служебную и коммерческую тайну

Необходимые основы закрепленные в технической документации с учетом действующих нормативных и методических документов в области информационной безопасности, а так же алгоритмы решения типовых задач обеспечения информационной безопасности и к применению программных средств системного, прикладного и специального назначения

Уметь:

применять базовые методы анализа изучаемых явлений, процессов и проектных решений и использовать основные требования закрепленные в законах и подзаконных актов, при разработки IT- технологий требующих правовых решений в ситуациях, возникающих вследствие нарушения основных законных интересов граждан и организаций

проводить базовый анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов и проводить эксперименты по заданной методике, осуществлять обработку результатов, оценку погрешности и определять достоверность получаемых результатов

осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения основ кибербезопасности и способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью

Владеть:

навыками проведения экспериментов по заданной методике, осуществлять обработку результатов, оценку погрешности и определять достоверность получаемых результатов; способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения основ кибербезопасности

базовыми навыками, позволяющими разрабатывать предложения по совершенствованию основ системы управления информационной безопасностью и формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью

базовыми методом проведения анализа информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов и способностью проводить эксперименты по заданной методике, осуществлять обработку результатов, оценку погрешности и определять достоверность получаемых результатов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем	Вид занятий	Семестр / Курс	Часов	Интеракт.
	Раздел 1. Специфика технологии защищенного документооборота. Методологические рекомендации по анализу режимов работы кибернетических систем	Раздел			
1.1	Задачи кибербезопасности в автоматизированных системах	Лек	6	2	1
1.2	Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз	Ср	6	4	0
1.3	Основы файловой системы Требования к системам защиты информации.	Лек	6	4	1
1.4	Лабораторная работа №1	Лаб	6	4	1

1.5	Общая характеристика сетей и протоколов передачи данных	Ср	6	8	0
1.6	Лабораторная работа №2	Лаб	6	4	0
1.7	Антивирусы и защита электронного документооборота от не санкционированного доступа	Ср	6	4	0
	Раздел 2. Раздел 2. Принципы построения системы кибербезопасности. Определение уязвимостей автоматизированных систем и выбор средств защиты. Формирование требований к построению систем криптографической и стеганографической защиты.	Раздел			
2.1	Хэш-функция и электронная подпись и протоколы электронных данных	Лек	6	4	0
2.2	Общие требования к паролям. Симметричное и асимметричное шифрование	Ср	6	8	0
2.3	Защищенные каналы данных облачные технологии и защищённый документооборот	Лек	6	4	1
2.4	Лабораторная работа №3	Лаб	6	6	2
2.5	Нормативно-правовые акты и стандарты по кибербезопасности	Ср	6	8	0
2.6	Преступления в сфере информационных технологий	Лек	6	4	1
2.7	Рубежный контроль	Лаб	6	4	1
2.8	Промежуточный контроль	Зачёт	6	4	0

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине "Основы кибербезопасности" рассмотрены и одобрены на заседании кафедры от «23» апреля 2019г. протоколом № 11, является приложением к рабочей программе.

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточного контроля по дисциплине "Основы кибербезопасности" рассмотрены и одобрены на заседании кафедры от «23» апреля 2019г. протоколом № 11, является приложением к рабочей программе.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Заглавие	Эл. адрес	Кол-
Л1.1	Загинайлов Ю. Н. - Теория информационной безопасности и методология защиты информации - М.|Берлин: Директ-Медиа, 2015.	http://biblioclub.ru/index.php?page=book&id=276557	1
Л1.2	Загинайлов Ю. Н. - Основы информационной безопасности: курс визуальных лекций - М.|Берлин: Директ-Медиа, 2015.	http://biblioclub.ru/index.php?page=book&id=362895	1

6.1.2. Дополнительная литература

	Заглавие	Эл. адрес	Кол-
Л2.1	Шаньгин В. Ф. - Информационная безопасность и защита информации: учебное пособие - Москва: ДМК Пресс, 2014.	http://www.iprbookshop.ru/29257	1
Л2.2	Прохорова О. В. - Информационная безопасность и защита информации: Учебник - Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.	http://www.iprbookshop.ru/43183	1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Crypt-Online - http://crypt-online.narod.ru/
Э2	Online decrypt/encrypt too - https://www.tools4noobs.com/online_tools/encrypt/

Э3	Steganography Online - http://stylesuxx.github.io/steganography/
Э4	Image Steganography - https://incoherency.co.uk/image-steganography/
6.3.1 Перечень программного обеспечения	
7.3.1.1	Для ауд. 501:
7.3.1.2	Microsoft Windows XP Professional Проприетарное программное обеспечение.Open License: 47818817
7.3.1.3	Microsoft Office 2003 SuitesПроприетарное программное обеспечение.Open License: 41902857
7.3.1.4	Adobe Acrobat Reader DC Бесплатное программное обеспечение
7.3.1.5	Google Chrome Свободная лицензияBSD
7.3.1.6	7-Zip Свободная лицензия GNULGPL
7.3.1.7	Для ауд. 407:
7.3.1.8	Microsoft Windows 7 Professional Проприетарное программное обеспечение.Open License:47818817
7.3.1.9	Microsoft Office Professional Plus 2007 Проприетарное программное обеспечение.Open License: 43219389
7.3.1.10	7-Zip Свободная лицензия GNULGPL
7.3.1.11	AdobeAcrobatReaderDCБесплатное программное обеспечение
7.3.1.12	GoogleChrome Свободная лицензия BSD
7.3.1.13	Для ауд.303:
7.3.1.14	MicrosoftWindows 8 Договор№0344100007512000081 от 12 декабря 2012 года
7.3.1.15	Microsoft Office Professional Plus 2007 Проприетарное программное обеспечение.Open License: 43219389
7.3.1.16	7-Zip Свободная лицензия GNULGPL
7.3.1.17	AdobeAcrobatReaderDCБесплатное программное обеспечение
7.3.1.18	GoogleChrome Свободная лицензия BSD
6.3.2 Перечень информационных справочных систем	
7.3.2.1	- Электронная библиотечная система «Научная библиотека КГУ» http://www.lib.kursksu.ru/
7.3.2.2	- Электронная библиотечная система «Университетская библиотека онлайн» http://www.biblioclub.ru
7.3.2.3	- Электронно-библиотечная система IPRBooks http://www.iprbookshop.ru/
7.3.2.4	- Электронная библиотека Юрайт http://www.biblio-online.ru/
7.3.2.5	- Научная электронная библиотека http://elibrary.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Лекции: Учебная аудитория для проведения занятий лекционного типа, практических занятий, групповых и индивидуальных консультаций, текущего контроля, 305000, Курская область, г. Курск, ул. Радищева, д. № 29,501 оснащена: Парта первого ряда двухместная – 2 шт., Парта первого ряда трехместная – фанера – 9 шт., Парта последнего ряда двухместная – 2 шт., Парта последнего ряда одноместная – 1 шт., Парта последнего ряда трехместная – фанера – 8 шт., Парта среднего ряда двухместная – 6 шт., Парта среднего ряда одноместная – 1 шт., Парта среднего ряда трехместная – фанера – 26 шт., Доска аудиторная – 1 шт., Стол офисный угловой с приставнойтумбой– 1 шт., Переносной мультимедийный проектор OptomaDX 211 (DLP. 2500Lm.XGA.3500: 1– 1 шт., Мобильный ПК EMACHINESE510 – 1 шт.
7.2	Практические занятия: Лаборатория экономики (учебная аудитория для проведения занятий лекционного типа, практических занятий, групповых и индивидуальных консультаций, текущего контроля),305000, Курская область, г. Курск, ул. Радищева, д. № 29,407 оснащена: Доска аудиторная – 1 шт., Коммутатор – 1 шт., Рабочая станция – 12 шт., Стол компьютерный – 12 шт., Шкаф офисный глухой 850х400х2000 – 2 шт., Шкаф офисный для документов со стеклом 850х400х2000 – 1 шт., Шкаф офисный для документов со стеклом 850х400х2000 – 1 шт., Шкаф офисный для документов со стеклом 850х400х2000 – 1 шт., Трибуна – 1 шт., Стол ученический двухместный – 8 шт.,Стул полумягкий ERA к50 – 15 шт., Стул ученический – 12 шт., Жалюзи – 3 шт.
7.3	Самостоятельная работа:
7.4	Аудитория для самостоятельной работы студентов, 305000, Курская область, г. Курск, ул. Радищева, д. № 29, 303 оснащена: Комплекты столов и стульев – 55 шт., Моноблок (ASUS ET2220I) с доступом к сети Интернет – 28 шт.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Приступая к изучению курса, студентам рекомендуется ознакомиться с содержанием рабочей программы, с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками, имеющимся на кафедре.

Изучение дисциплины требует систематического и последовательного накопления знаний, поэтому студентам рекомендуется перед очередной лекцией просмотреть по конспекту материал предыдущей. При затруднениях в восприятии материала следует обращаться к основным литературным источникам, к лектору (по графику его консультаций) или к преподавателю на занятиях.

Самостоятельная работа студентов включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы.

К каждой теме учебной дисциплины подобрана основная и дополнительная литература.

Основная литература - это учебники и учебные пособия.

Дополнительная литература - это монографии, сборники научных трудов, журнальные и газетные статьи, различные справочники, энциклопедии, интернет ресурсы.

В начале изучения курса, в учебнике или учебном пособии, рекомендуемом в качестве основной или дополнительной литературы для освоения дисциплины, студенту рекомендуется проанализировать оглавление, научно-справочный аппарат, аннотацию и предисловие.

Студенту рекомендуется использовать следующие виды записей при работе с литературой:

Конспект - краткая схематическая запись основного содержания научной работы, целью которой является не переписывание материала, а выявление его логики, системы доказательств, основных выводов. Тезисы - концентрированное изложение основных положений прочитанного материала.

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

Для изучения конспекта лекции в тот же день, после лекции студенту рекомендуется 10-15 минут.

Изучение конспекта лекции по предыдущей теме за день перед лекцией по следующей темой - 10-15 минут.

Изучение теоретического материала по учебнику и конспекту - 1 час в неделю.

Подготовка к лабораторному занятию - 30 мин.

Всего в неделю - 2 часа 55 минут.

При изучении дисциплины рекомендуется самостоятельно изучать материал, который еще не прочитан на лекции. В этом случае, понимание лекционного материала осуществляется студентом более эффективно.

Для понимания материала и качественного его усвоения рекомендуется следующая последовательность действий:

После работы на лекции, или на лабораторной работе, и после окончания учебных занятий, студенту рекомендуется самостоятельно проанализировать лекционный материал, или материал лабораторной работы (10-15 минут).

При подготовке к лекции, или лабораторной работе по следующей теме, студенту рекомендуется проанализировать лекционной материал, или материал лабораторной работы по предыдущей теме (10-15 минут).

При подготовке к лабораторным занятиям рекомендуется также изучить соответствующий теоретический материал по основам кибербезопасности, предусмотренный темой лабораторной работы.

В течение учебной недели студенту рекомендуется изучать материал по основам кибербезопасности, изложенный в рекомендуемой литературе в течение 1 часа.