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
Кибербезопасность в научной деятельности

Направление подготовки: 06.06.01 БИОЛОГИЧЕСКИЕ НАУКИ

Профиль подготовки: Ботаника

Квалификация: Исследователь. Преподаватель-исследователь

Форма обучения: заочная

Общая трудоемкость 2 ЗЕТ

Виды контроля в семестрах:

зачет(ы) 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	19			
Вид занятий	УП	РП	УП	РП
Лекции	2	2	2	2
Лабораторные	8	8	8	8
Итого ауд.	10	10	10	10
Контактная работа	10	10	10	10
Сам. работа	58	58	58	58
Часы на контроль	4	4	4	4
Итого	72	72	72	72

Курск 2019

Рабочая программа дисциплины Кибербезопасность в научной деятельности / сост. ; Курск. гос. ун-т. - Курск, 2019. - с.

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Минобрнауки России от 30.07.2014 г. № 871 "Об утверждении ФГОС ВО по направлению подготовки 06.06.01 БИОЛОГИЧЕСКИЕ НАУКИ (уровень аспирантуры)"

Рабочая программа дисциплины "Кибербезопасность в научной деятельности" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 06.06.01 БИОЛОГИЧЕСКИЕ НАУКИ профиль

Составитель(и):

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Заложить методологию обеспечения кибербезопасности информационных систем и информационных ресурсов, используемых в профессиональной деятельности

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

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

ОПК-1: способность самостоятельно осуществлять научно-исследовательскую деятельность в соответствующей профессиональной области с использованием современных методов исследования и информационно-коммуникационных технологий

Знать:

Основные понятия и содержание технологий обеспечения 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.

Понятия комплекс мер по обеспечению 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 государственную 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 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 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 кибербезопасности и способность разрабатывать предложения по совершенствованию системы управления информационной безопасность

Владеть:

знаниями, позволяющими сформировать представление о механизмах 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 кибербезопасности

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

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	7	1	0

1.2	Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз	Ср	7	8	0
1.3	Основы файловой системы Требования к системам защиты информации.	Ср	7	6	0
1.4	Лабораторная работа №1	Лаб	7	2	0
1.5	Общая характеристика сетей и протоколов передачи данных	Ср	7	8	0
1.6	Антивирусы и защита электронного документооборота от не санкционированного доступа	Ср	7	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	7	1	0
2.2	Общие требования к паролям. Симметричное и асимметричное шифрование	Ср	7	4	0
2.3	Лабораторная работа №2	Лаб	7	2	0
2.4	Защищенные каналы данных облачные технологии и защищённый документооборот	Ср	7	8	0
2.5	Лабораторная работа №3	Лаб	7	2	0
2.6	Нормативно-правовые акты и стандарты по кибербезопасности	Ср	7	10	0
2.7	Преступления в сфере информационных технологий	Ср	7	10	0
2.8	Рубежный контроль	Лаб	7	2	0
2.9	Промежуточный контроль	Зачёт	7	4	0

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине "Кибербезопасность в научной деятельности" были рассмотрены и одобрены на заседании кафедры "Математического анализа и прикладной математики " от 13 апреля 2017 г., протокол №7

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточного контроля по дисциплине "Кибербезопасность в научной деятельности" были рассмотрены и одобрены на заседании кафедры "Математического анализа и прикладной математики " от 13 апреля 2017 г., протокол №7

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	Steganography Online:http://stylesuxx.github.io/steganography/-http://stylesuxx.github.io/steganography/		
Э2	Image Steganography:https://incoherency.co.uk/image-steganography/-https://incoherency.co.uk/image-steganography/		
Э3	Online decrypt/encrypt tool :https://www.tools4noobs.com/online_tools/encrypt/-https://www.tools4noobs.com/online_tools/encrypt/		
Э4	Crypt-Online:http://crypt-online.narod.ru/-http://crypt-online.narod.ru/		
6.3.1 Перечень программного обеспечения			
7.3.1.1	209:		
7.3.1.2	Microsoft Windows 7 (Open License: 47818817)		
7.3.1.3	Microsoft Office Professional 2007 (Open License: 43219389)		
7.3.1.4	Adobe Acrobat Reader DC (Бесплатное программное обеспечение)		
7.3.1.5	7-Zip (Свободная лицензия GNU LGPL)		
7.3.1.6	Google Chrome (Свободная лицензия BSD)		
7.3.1.7			
7.3.1.8	199:		
7.3.1.9	Microsoft Windows 7 (Open License: 47818817)		
7.3.1.10	Microsoft Office Professional 2007 (Open License: 43219389)		
7.3.1.11	Adobe Acrobat Reader DC (Бесплатное программное обеспечение)		
7.3.1.12	7-Zip (Свободная лицензия GNU LGPL)		
7.3.1.13	Google Chrome (Свободная лицензия BSD)		
7.3.1.14	Зоркий Глаз (Проприетарное условно-бесплатное программное обеспечение)		
7.3.1.15	PDF Creator (Свободное программное обеспечение AGPL)		
7.3.1.16	Recuva FREE (Проприетарное условно-бесплатное программное обеспечение)		
7.3.1.17	USB Flash Security (Условно-бесплатное программное обеспечение)		
7.3.1.18	Easy File Locker (Проприетарное условно-бесплатное программное обеспечение)		
7.3.1.19			
7.3.1.20	146:		
7.3.1.21	Microsoft Windows 7 (Open License: 47818817)		
7.3.1.22	Microsoft Office Professional 2007 (Open License: 43219389)		
7.3.1.23	Adobe Acrobat Reader DC (Бесплатное программное обеспечение)		
7.3.1.24	7-Zip (Свободная лицензия GNU LGPL)		
7.3.1.25	Google Chrome (Свободная лицензия BSD)		
6.3.2 Перечень информационных справочных систем			
7.3.2.1	ЭБС КГУ http://library-reader.kursksu.ru/		
7.3.2.2	ЭБС "IPRBooks" http://www.iprbookshop.ru/		

7.3.2.3	ЭБС "Юрайт" https://www.biblio-online.ru/
7.3.2.4	ЭБС "Университетская бибилотечная система Online" http://biblioclub.ru/
7.3.2.5	Электронная библиотека.- Режим доступа: http://elibrary.ru
7.3.2.6	http://base.consultant.ru

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, груп-повых и Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, груп-повых и индивидуальных консультаций, текущего контроля и промежуточной аттестации,
7.2	305000,Курская область г. Курск, ул. Радищева,д. №33, 209.
7.3	Комплекты учебных столов и стульев (28 шт)
7.4	Доска ученическая (настенная) – 1 шт.
7.5	Мультимедиа-проектор – 1 шт.
7.6	
7.7	Лаборатория программно-аппаратных средств обеспечения информационной безопасности;
7.8	Лаборатория технических средств защиты информации;
7.9	для проведения занятий лекционного типа, занятий семинаркого типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы,
7.10	305000, Курская область, г. Курск, ул. Радищева, д. №33, 199.
7.11	Моноблок LenovoC560 – 9 шт.
7.12	Стенд информационный 1,4м*0,9м – 9 шт.
7.13	Малогабаритный камуфлирован-ный блокиратор работы сотовых телефонов и закладных устройств – 1 шт.
7.14	Селективный обнаружитель циф-ровых радиоустройств ST062 – 1 шт.
7.15	Устройство защиты объектов ин-форматизации от утечки инфор-мации за счет ПЭМИН «Блокада» – 1 шт.
7.16	Нелинейный локатор «Буклет-2» – 1 шт.
7.17	Устройство МП—1А – 1 шт.
7.18	Электронно-оптическое устройст-во для обнаружения любых типов оптических устройств «Гранат» – 1 шт.
7.19	Программно-аппаратный ком-плекс «Соболь» – 1 шт.
7.20	ИМФ-3 имитатор многофункцио-нальный – 1 шт.
7.21	МониторЖК-панель 17 Асер – 1 шт.
7.22	Жалюзи вертикальные тканевые – 1 шт.
7.23	Концентратор 24порт – 1 шт.
7.24	Лабораторный комплекс «Беспро-водные сети ЭВМ»
7.25	Система активной защиты рече-вой акустической информации SEL-157 "Шагрень",
7.26	Устройство «Смарт (Комплекс оценки эффективности защиты речевой информации от утечки по акустическому, виброакустиче-скому и акустоэлектрическому каналам),
7.27	Программно-аппаратные средства защиты информации от НСД .
7.28	
7.29	Помещение для самостоятельной работы обучающихся – читальный зал, оснащенный компьютерной техникой с возможностью подключения к сети "Интернет" и с обеспечением доступа в электронную информационно-образовательную среду университета
7.30	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 146.
7.31	Столов – 61
7.32	Посадочных мест – 162
7.33	Компьютеров:
7.34	Для пользователей – 40
7.35	Для библиотекаря – 2
7.36	Моноблоков MSI (27) - модель MS-A912, 2гб оперативной памя-ти, Athlon CPU D525 1.80GHz
7.37	Моноблоков Asus (13) - модель ET2220I, 4гб оперативной памяти, Intel Core i3-3220 CPU 3.30 GHz

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

1. Методические указания по освоению дисциплины (модуля)
Студентам необходимо ознакомиться с содержанием рабочей программы, с целями и задачами дисциплины, ее связями с

другими дисциплинами образовательной программы, методическими разработками, имеющимся на кафедре.
1.1. Указания по подготовке к занятиям лекционного типа
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 семинарского типа.

1.2. Методические указания по выполнению самостоятельной работы

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, которые содержатся в «Методических указаниях по самостоятельной работе по дисциплине «Кибербезопасность» утвержденных на заседании кафедры от «24» апреля 2016 г. протокол № 9.

1.3. Методические указания по работе с литературой
Следует характеризовать структуру рекомендуемой литературы:
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 учебнике/ учебном пособии следует ознакомиться с оглавлением и научно-справочным аппаратом, прочитать аннотацию и предисловие. Целесообразно ее пролистать, рассмотреть иллюстрации, таблицы, диаграммы, приложения. Такое поверхностное ознакомление позволит узнать, какие главы следует читать внимательно, а какие прочитать быстро.
Студенту следует использовать следующие виды записей при работе с литературой:
Конспект - краткая схематическая запись основного содержания научной работы. Целью является не переписывание произведения, а выявление его логики, системы доказательств, основных выводов. Тезисы - концентрированное изложение основных положений прочитанного материала.
1. Планирование и организация времени, необходимого для изучения дисциплины.
Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:
Изучение конспекта лекции в тот же день, после лекции - 10-15 минут.
Изучение конспекта лекции за день перед следующей лекцией - 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.
2. Описание последовательности действий студента («сценарий изучения дисциплины»).
При изучении дисциплины очень полезно самостоятельно изучать материал, который еще не прочитан на лекции. Тогда лекция будет гораздо понятнее. Однако легче при изучении курса следовать изложению материала на лекции. Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:
1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня (10-15 минут).
2. При подготовке к лекции следующего дня, нужно просмотреть текст предыдущей лекции, подумать о том, какая может быть тема следующей лекции (10-15 минут).
3. В течение недели выбрать время (1 час) для работы с литературой по криптографическим методам в биб-лиотеке или изучить дополнительную литературу в электронной форме.
3. Методические рекомендации по подготовке лабораторные занятий.
По данному курсу предусмотрены лабораторные занятия. При подготовке к лабораторным занятиям следует изучить соответствующий теоретический материал по криптографическим методам и, если предусмотрено темой, изучить работу программ-калькуляторов или функций криптографического модуля Python.
Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги по криптоанализу. Литературу по курсу рекомендуется изучать в библиотеке. Полезно использовать несколько учебников. Однако легче освоить курс, придерживаясь одного учебника и конспекта. Рекомендуется, кроме «заучивания» материала, добиться состояния понимания изучаемой темы дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько простых упражнений на данную тему. Кроме того, очень полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): о чем этот параграф?, какие новые понятия вве-дены, каков их смысл?, какие математические принципы используются в этом параграфе и каков их смысл «своими словами»?. Сами криптографические алгоритмы следует не заучивать, а «понять». С этой целью рекомендуется записать идею алгоритма, составить план преобразования открытого текста в шифртекст и обратно, сравнить используемые алгоритмы и теоремы в конспекте и в учебнике. При изучении теоретического материала всегда нужно рисовать схемы или графики.
4. Рекомендации по работе с литературой.
5. Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги по криптографии и криптоанализу. Литературу по курсу рекомендуется изучать в библиотеке. Полезно использовать несколько учебников по изучаемому курсу.