МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
"Курский государственный университет"

Кафедра информационной безопасности

УТВЕРЖДЕНО

протокол заседания
Ученого совета от 31.08.2016 г., №1

Рабочая программа дисциплины
Кибербезопасность

Направление подготовки: 45.04.02 Лингвистика

Профиль подготовки: Иностранный язык и межкультурная коммуникация

Квалификация: магистр

Кафедра иностранных языков и профессиональной коммуникации

Форма обучения: очная

Общая трудоемкость 2 ЗЕТ

Виды контроля в семестрах:

зачет(ы) 4

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		Итого	
Недель	14			
Вид занятий	УП	РП	УП	РП
Лекции	14	14	14	14
Лабораторные	14	14	14	14
Итого ауд.	28	28	28	28
Контактная работа	28	28	28	28
Сам. работа	44	44	44	44
Итого	72	72	72	72

Курск 2017

Рабочая программа дисциплины Кибербезопасность / сост. ; Курск. гос. ун-т. - Курск, 2017. - с.

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Минобрнауки России от 1 июля 2016 г. № 783 "Об утверждении ФГОС ВО по направлению подготовки 45.04.02 Лингвистика (уровень магистратуры)" (Зарегистрировано в Минюсте России 18 июля 2016 г. № 42896)

Рабочая программа дисциплины "Кибербезопасность" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 45.04.02 Лингвистика профиль Иностранный язык и межкультурная коммуникация

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

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ОПК-17: владением современной информационной и библиографической культурой
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 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 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 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;
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. Введение.	Раздел			
1.1	Задачи кибербезопасности в автоматизированных системах.	Лек	4	2	0
1.2	Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз.	Лек	4	2	0
1.3	Лабораторная работа №1.	Лаб	4	2	0
1.4	Основы файловой системы Требования к системам защиты информации.	Ср	4	12	0
1.5	Лабораторная работа №2.	Лаб	4	2	0
	Раздел 2. Специфика технологии защищенного документооборота - Методологические рекомендации по анализу режимов работы кибернетических систем.	Раздел			

2.1	Компьютерные вирусы как угроза кибербезопасности. Их классификация.	Лек	4	2	0
2.2	Антивирусы и защита электронного документооборота от не санкционированного доступа.	Лек	4	2	0
2.3	Лабораторная работа №3.	Лаб	4	2	0
2.4	Общая характеристика сетей и протоколов передачи данных.	Ср	4	4	0
2.5	Лабораторная работа №4.	Лаб	4	2	0
	Раздел 3. Принципы построения системы кибербезопасности. Определение уязвимостей автоматизированных систем и выбор средств защиты. Формирование требований к построению систем криптографической и стеганографической защиты.	Раздел			
3.1	Общие требования к паролям симметричное и асимметричное шифрование.	Лек	4	2	0
3.2	Лабораторная работа №5.	Лаб	4	2	0
3.3	Хэш-функция и электронная подпись и протоколы электронных данных.	Лек	4	2	0
3.4	Защищенные каналы данных облачные технологии и защищённый документооборота.	Ср	4	14	0
3.5	Лабораторная работа №6.	Лаб	4	2	0
	Раздел 4. Киберпреступность и способы её предотвращения.	Раздел			
4.1	Нормативно-правовые акты и стандарты по кибербезопасности.	Лек	4	2	0
4.2	Преступления в сфере информационных технологий.	Ср	4	12	0
4.3	Рубежный контроль.	Лаб	4	2	0
4.4	Промежуточная аттестация.	Зачёт	4	2	0

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине «Кибербезопасность» рассмотрены и одобрены на заседании кафедры математического анализа и прикладной математики «29» августа 2016 г. протокол № 1 и являются приложением к рабочей программе.

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточной аттестации по дисциплине «Кибербезопасность» рассмотрены и одобрены на заседании кафедры математического анализа и прикладной математики «29» августа 2016 г. протокол № 1 и являются 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-

	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
Л2.3	Нестеров С. А. - Основы информационной безопасности: учебное пособие - Санкт-Петербург: Издательство Политехнического университета, 2014.	http://biblioclub.ru/index.php?page=book&id=363040	1
Л2.4	Сердюк В. А. - Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие - Москва: Издательский дом Высшей школы экономики, 2015.	http://biblioclub.ru/index.php?page=book&id=440285	1

6.1.3. Методические разработки

	Заглавие	Эл. адрес	Кол-
Л3.1	Крыжевич Л. С. - Информационная безопасность: учеб.-метод. пособие для студ. ФФМИ Курск. гос. ун-та - Курск: [б. и., 2015].		1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Steganography Online : http://stylesuxx.github.io/steganography/
Э2	Image Steganography : https://incoherency.co.uk/image-steganography/
Э3	Online encrypt tool : https://www.tools4noobs.com/online_tools/encrypt/
Э4	Crypt-Online : 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	199:
7.3.1.8	Microsoft Windows 7 Professional (Open License: 47818817)
7.3.1.9	Microsoft Office Professional 2007 (Open License: 43219389)
7.3.1.10	Adobe Acrobat Reader DC (Бесплатное программное обеспечение)
7.3.1.11	7-Zip (Свободная лицензия GNU LGPL)
7.3.1.12	Google Chrome (Свободная лицензия BSD)
7.3.1.13	Зоркий глаз (Проприетарное условно-бесплатное программное обеспечение)
7.3.1.14	PDF Creator (Свободное программное обеспечение AGPL)
7.3.1.15	Easy File Locker (Проприетарное условно-бесплатное программное обеспечение)
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	146:
7.3.1.19	Microsoft Windows 7 Professional (Open License: 47818817)
7.3.1.20	Microsoft Windows 8 (Договор №0344100007512000081 от 12 декабря 2012 года)
7.3.1.21	Microsoft Office Professional Plus 2007 (Open License: 43219389)
7.3.1.22	7-Zip (Свободная лицензия GNU LGPL)

7.3.1.23	Adobe Acrobat Reader DC (Бесплатное программное обеспечение);
7.3.1.24	Google Chrome (Свободная лицензия BSD)
7.3.1.25	
7.3.1.26	Adobe Acrobat Reader DC (Бесплатное программное обеспечение)
7.3.1.27	7-Zip (Свободная лицензия GNU LGPL)
7.3.1.28	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	Научная электронная библиотека eLIBRARY.RU - http://elibrary.ru
7.3.2.6	Справочная правовая система "КонсультантПлюс" - http://base.consultant.ru

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.
7.2	305000, Курская область, г. Курск, ул. Радищева, д. №33, 209
7.3	Парта – 32 шт.
7.4	Стул – 65 шт.
7.5	Мобильный ПК ASUS X553S – 1 шт.
7.6	Мультимедиа-проектор – 1 шт.
7.7	Экран мультимедийный – 1 шт.
7.8	Доска ученическая (настенная) – 1 шт.
7.9	Жалюзи – 4 шт.
7.10	Вешалка – 3 шт.
7.11	
7.12	Лаборатория технической защиты информации, Лаборатория программно-аппаратных средств обеспечения информационной безопасности.
7.13	305000, Курская область, г. Курск, ул. Радищева, д. №33, 199.
7.14	Моноблок (Lenovo C560) – 9 шт.
7.15	Стенд информационный 1,4м*0,9м – 9 шт.
7.16	Малогабаритный камуфлированный блокиратор работы сотовых телефонов и закладных устройств – 1 шт.
7.17	Селективный обнаружитель цифровых радиоустройств ST062 – 1 шт.
7.18	Устройство защиты объектов информатизации от утечки информации за счет ПЭМИН «Блокада» – 1 шт.
7.19	Нелинейный локатор «Буклет-2» – 1 шт.
7.20	Устройство МП—1А – 1 шт.
7.21	Электронно-оптическое устройство для обнаружения любых типов оптических устройств «Гранат» – 1 шт.
7.22	Программно-аппаратный комплекс «Соболь» – 1 шт.
7.23	ИМФ-3 имитатор многофункциональный – 1 шт.
7.24	Монитор ЖК-панель 17 Асер – 1 шт.
7.25	Жалюзи вертикальные тканевые – 2 шт.
7.26	Концентратор 24порт – 1 шт.
7.27	Парта – 9 шт.
7.28	Стол комп. – 12 шт.
7.29	Стул – 17 шт.
7.30	Доска с механизмом – 1 шт.
7.31	Стенд учебный лабораторный комплекс SDX-0,9 – 3 шт.

7.32	Стенд учебный лабораторный комплекс SDK-6,1 – 4 шт.
7.33	Стенд учебный лабораторный комплекс SDK-7 – 4 шт.
7.34	Стенд учебный лабораторный комплекс SDK-1.1 – 6 шт.
7.35	Стенд учебный лабораторный комплекс SDK-5.0 – 7 шт.
7.36	Устройство «Смарт» (на базе СКМ-21) (Комплекс оценки эффективности защиты речевой информации от утечки по акустическому, виброакустическому и акустоэлектрическому каналам) – 1 шт.
7.37	Система активной защиты речевой акустической информации SEL-157 "Шагрень" – 1 шт.
7.38	Программно-аппаратные средства защиты информации от НСД (Электронные идентификаторы Рутокен) – 1 шт.
7.39	Лабораторный комплекс «Беспроводные сети» УП-134 – 1 шт.
7.40	
7.41	Учебная аудитория для самостоятельной работы.
7.42	305000, Курская область, г. Курск, ул. Радищева, д. №33, 146
7.43	Учебная мебель: стол – 61 шт.; стул – 162 шт.
7.44	Моноблок (MSI MS-A912) – 27 шт.
7.45	Моноблок (ASUS ET2220I) – 13 шт.
7.46	

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 кибербезопасности, предусмотренный темой лабораторной работы.

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