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 30.08.2017 г., №1

Рабочая программа дисциплины
Кибербезопасность

Направление подготовки: 38.04.02 Менеджмент

Профиль подготовки: Управление организацией

Квалификация: магистр

Факультет экономики и менеджмента

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	7			
Вид занятий	УП	РП	УП	РП
Лекции	6	6	6	6
Лабораторные	6	6	6	6
Итого ауд.	12	12	12	12
Контактная работа	12	12	12	12
Сам. работа	60	60	60	60
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 30 марта 2015 г. № 322 "Об утверждении ФГОС ВО по направлению подготовки 38.04.02 Менеджмент (уровень магистратуры)" (Зарегистрировано в Минюсте России 15 апреля 2015 г. № 36854)

Рабочая программа дисциплины "Кибербезопасность" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 38.04.02 Менеджмент профиль Управление организацией

Составитель(и):

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Заложить методологию обеспечения кибербезопасности информационных систем и информационных ресурсов, используемых в профессиональной деятельности
1.2	

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

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ОК-3: готовностью к саморазвитию, самореализации, использованию творческого потенциала
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
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
уеобходимые 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 решения и поиска необходимых процессов в управлении информационной безопасностью защищаемых объектов, а также поиском и применением нормативно-правовой базы для решения конкретных задач обеспечения законности в сфере информационной безопасности.
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. 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	1	0
1.4	Основы файловой системы Требования к системам защиты информации.	Ср	4	4	0
1.5	Лабораторная работа №2	Лаб	4	1	0
1.6	Общая характеристика сетей и протоколов передачи данных	Ср	4	8	0

1.7	Антивирусы и защита электронного документооборота от не санкционированного доступа	Ср	4	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	Антивирусы и защита электронного документооборота от не санкционированного доступа	Лек	4	2	0
2.2	Общие требования к паролям симметричное и асимметричное шифрование	Ср	4	4	0
2.3	Лабораторная работа №3	Лаб	4	1	0
2.4	Хэш-функция и электронная подпись и протоколы электронных данных	Ср	4	8	0
2.5	Защищенные каналы данных облачные технологии и защищённый документооборот	Ср	4	8	0
2.6	Лабораторная работа №4	Лаб	4	1	0
	Раздел 3. Раздел 3. Киберпреступность и способы её предотвращения	Раздел			
3.1	Нормативно-правовые акты и стандарты по кибербезопасности	Ср	4	12	0
3.2	Преступления в сфере информационных технологий	Ср	4	10	0
3.3	Рубежный контроль	Лаб	4	2	0
3.4	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 13.04.2017 протокол №7 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 13.04.2017 протокол №7 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-
Л2.1	Шаньгин В. Ф. - Информационная безопасность и защита информации: учебное пособие - Москва: ДМК Пресс, 2014.	http://www.iprbookshop.ru/29257	1

	Заглавие	Эл. адрес	Кол-
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

6.1.3. 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	Online encrypt tool ; https://www.tools4noobs.com/online_tools/encrypt/
Э3	Image Steganography ; https://incoherency.co.uk/image-steganography/
Э4	Crypt-Online ; http://crypt-online.narod.ru/

6.3.1 Перечень программного обеспечения

7.3.1.1	Лаборатория технологий управления и торгового дела №505:
7.3.1.2	MicrosoftWindows 7 Prof проприетарное программное обеспечение. OpenLicense: 47818817;
7.3.1.3	Microsoft Office Professional Plus 2007 проприетарное программное обеспечение. OpenLicense: 43219389;
7.3.1.4	Google Chrome свободная лицензия BSD;
7.3.1.5	7-Zip свободная лицензия GNULGPL;
7.3.1.6	Adobe Acrobat Reader DC бесплатное программное обеспечение;
7.3.1.7	Microsoft Windows XP Professional проприетарное программное обеспечение. Open License: 47818817;
7.3.1.8	Microsoft Office Professional 2003 проприетарноепрограммноеобеспечение. Open License: 41902857.
7.3.1.9	
7.3.1.10	Помещение для самостоятельной работы обучающихся – аудитория №303:
7.3.1.11	Microsoft Windows 8 (Договор №0344100007512000081 от 12 декабря 2012 года);
7.3.1.12	Microsoft Office Professional Plus 2007 проприетарное программное обеспечение. Open License: 43219389;
7.3.1.13	7-Zip свободная лицензия GNU LGPL;
7.3.1.14	Adobe Acrobat Reader DC бесплатное программное обеспечение;
7.3.1.15	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	Лаборатория технологий управления и торгового дела №505
7.2	(305000, Курская область, г. Курск, ул. Радищева, д. №29)
7.3	(учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ)),
7.4	оснащена:
7.5	доска магнитно-маркерная 90*120 PROFF WB0912/20-0702 (с магнитом и маркером) – 1 шт.;
7.6	доска информационная – 1 шт.;
7.7	концентратор Switch24 port COMPEX – 1 шт.;
7.8	стол офисный угловой с подкатной тумбой 140*140/65*75 – 1 шт.;
7.9	стол компьютерный 103*67*75 – 11 шт.;

7.10	кресло рабочее поворотно-подъемное Chairman CH 661 – 13 шт.;
7.11	рабочая станция – 12 шт.;
7.12	стул полумягкий ERA – 4 шт.;
7.13	мобильный ПК EMACHINESE 510 – 1 шт.;
7.14	переносной мультимедийный проектор Optoma DX 211 DLP. 2500Lm.XGA.3500: 1 – 1 шт.
7.15	
7.16	Помещение для самостоятельной работы обучающихся – аудитория №303
7.17	(305000, Курская область, г. Курск, ул. Радищева, д. №29),
7.18	оснащенная компьютерной техникой с возможностью подключения к сети "Интернет" и с обеспечением доступа в электронную информационно-образовательную среду университета,
7.19	оснащена:
7.20	стол – 55 шт.;
7.21	стул – 55 шт.;
7.22	моноблоков (ASUS ET2220I) – 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 кибербезопасности, предусмотренный темой лабораторной работы.

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