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 29.04.2019 г., №9

Рабочая программа дисциплины
Кибербезопасность

Направление подготовки: 20.04.01 ТЕХНОСФЕРНАЯ БЕЗОПАСНОСТЬ

Профиль подготовки: Управление и аудит в техносферной безопасности

Квалификация: магистр

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	6,3			
Вид занятий	УП	РП	УП	РП
Лекции	6	6	6	6
Лабораторные	12	12	12	12
Итого ауд.	18	18	18	18
Контактная работа	18	18	18	18
Сам. работа	54	54	54	54
Итого	72	72	72	72

Курск 2019

Рабочая программа дисциплины Кибербезопасность / сост. к.т.н, Доцент, Гордиенко В.В.; Курск. гос. ун-т. - Курск, 2019. - с.

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Минобрнауки России от 06.03.2015 г. № 172 "Об утверждении ФГОС ВО по направлению подготовки 20.04.01 ТЕХНОСФЕРНАЯ БЕЗОПАСНОСТЬ (уровень магистратуры)"

Рабочая программа дисциплины "Кибербезопасность " предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 20.04.01 ТЕХНОСФЕРНАЯ БЕЗОПАСНОСТЬ профиль Управление и аудит в техносферной безопасности

Составитель(и):

к.т.н, Доцент, Гордиенко В.В.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Сформировать навыки обеспечения безопасности информационных систем и информационных ресурсов, используемых в профессиональной деятельности, от вредоносного воздействия, направленного на нарушение или прекращение их функционирования.
1.2	

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

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-10: способностью анализировать, оптимизировать и применять современные информационные технологии при решении научных задач
Знать:
основные способы анализа и оптимизации технологических процессов с применением современных информационных технологий и учетом требований кибербезопасности
Уметь:
осуществлять поиск уязвимостей в системах безопасности и минимизировать риски от целенаправленных атак на информационные ресурсы
Владеть:
инструментами анализа и методами оптимизации технологических процессов с применением современных информационных технологий области решения профессиональных задач в научной деятельности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем	Вид занятий	Семестр / Курс	Часов	Интерак.	Часы на пр. подгот.
	Раздел 1. Задачи кибербезопасности в автоматизированных системах	Раздел				
1.1	Определение уязвимостей автоматизированных систем и выбор средств защиты.	Лек	4	2	0	0
1.2	Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз	Ср	4	2	0	0
1.3	Разграничение прав доступа в информационных системах	Лаб	4	2	0	0
1.4	Основы файловой системы. Требования к системам защиты информации.	Ср	4	10	0	0
1.5	Защита файловых систем от несанкционированного доступа	Лаб	4	2	0	0
1.6	Общая характеристика сетей и протоколов передачи данных	Ср	4	10	0	0
1.7	Антивирусы и защита электронного документооборота от несанкционированного доступа	Ср	4	6	0	0
	Раздел 2. Раздел 2. Принципы построения системы кибербезопасности. Формирование требований к построению систем криптографическиой и стеганографической защиты.	Раздел				
2.1	Общие требования к паролям симметричное и асимметричное шифрование	Лек	4	2	0	0

2.2	Защищенные каналы передачи данных, облачные технологии и защищённый документооборот	Ср	4	6	0	0
2.3	Формироваиние требований к ключам асимметричного шифрования при передаче данных	Лаб	4	2	0	0
2.4	Хэш-функция, электронная подпись и криптографические протоколы	Ср	4	8	0	0
2.5	Методы реагирования на инциденты кибербезопасности	Лаб	4	2	0	0
	Раздел 3. Раздел 3. Киберпреступность и способы её предотвращения	Раздел				
3.1	Нормативно-правовые акты и стандарты по кибербезопасности	Лек	4	2	0	0
3.2	Формирование правовых документов по хранению, обработке персональных данных на предприятии	Лаб	4	2	0	0
3.3	Преступления в сфере информационных технологий	Ср	4	10	0	0
3.4	Определение категории значимости объектов критической инфраструктуры	Лаб	4	2	0	0
3.5	Промежуточная аттестация	Зачёт	4	2	0	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 информационной безопасности от «18» апреля 2019 г. протоколом № 9, является 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 информационной безопасности от «18» апреля 2019 г. протоколом № 9, 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-во
Л1.1	Филиппов Б. И., Шерстнева О. Г. - Информационная безопасность. Основы надежности средств связи: учебник - Москва, Берлин: Директ-Медиа, 2019.	https://biblioclub.ru/index.php?page=book&id=499170	1
Л1.2	Басыня Е. А. - Системное администрирование и информационная безопасность: учебное пособие - Новосибирск: Новосибирский государственный технический университет, 2018.	https://biblioclub.ru/index.php?page=book&id=575325	1
Л1.3	Шунейко А. А., Авдеенко И. А. - Информационная безопасность человека: учебное пособие - Москва: Владос, 2018.	https://biblioclub.ru/index.php?page=book&id=573372	1

6.1.2. Дополнительная литература

	Заглавие	Эл. адрес	Кол-во
Л2.1	Моргунов А. В. - Информационная безопасность: учебно-методическое пособие - Новосибирск: НГТУ, 2019.	https://e.lanbook.com/book/152227	1
Л2.2	- Информационная безопасность: лабораторный практикум - Пермь: ПГТПУ, 2018.	https://e.lanbook.com/book/129509	1

6.3.1 Перечень программного обеспечения

7.3.1.1	
7.3.1.2	Аудитории для самостоятельной работы (Р29/УК-303)и (Р33/ЛК-146)
7.3.1.3	305000, Курская область, г. Курск, ул. Радищева д. № 33
7.3.1.4	Программное обеспечение: Microsoft Windows 7 Professional Open License: 47818817 с 15.12.2010;

7.3.1.5	Microsoft Windows 8 ООО Техника и Сервис Договор №0344100007512000081 от 12 декабря 2012 года; Microsoft Office Professional Plus 2007 Open License:43219389 с 18.12.2007;
7.3.1.6	7-Zip Свободная лицензия GNU LGPL от 29 июня 2007
7.3.1.7	
7.3.1.8	Компьютерный класс (КМ53/УК-1301): Курск, ул. Карла Маркса, д. 53, Учебный корпус, Карла Маркса, д. 53
7.3.1.9	Программное обеспечение: Microsoft Windows 10 Pro Open License: 69186223,
7.3.1.10	Microsoft Office Professional 2007 Open License: 43219389 с 18.12.2007,
7.3.1.11	Audodesk Autocad 2010 проприетарное программное обеспечение бесплатная версия для образовательных учреждений,
7.3.1.12	7-Zip Свободная лицензия GNU LGPL от 29 июня 2007,
7.3.1.13	Adobe Acrobat Reader DC проприетарное программное обеспечение бесплатная версия,
7.3.1.14	Диполь (Гражданская оборона Виртуальный 3д тренажер Отработка действий в защитном сооружении ГО), сетевая версия Лицензионный договор 146/М от 11 декабря 2019,
7.3.1.15	Диполь (Гражданская оборона Виртуальный 3д тренажер Отработка действий по ведению радиационной, химической разведки), сетевая версия версия Лицензионный договор 146/М от 11 декабря 2019,
7.3.1.16	Диполь (Радиационная безопасность и Радиационный контроль) сетевая версия версия Лицензионный договор 146/М от 11 декабря 2019.
6.3.2 Перечень информационных справочных систем	
7.3.2.1	СС КонсультантПлюс;
7.3.2.2	Электронный Фонд правовой и нормативно-технической документации "Техэксперт"

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	
7.2	Аудитории для самостоятельной работы (Р29/УК-303)и (Р33/ЛК-146)
7.3	305000, Курская область, г. Курск, ул. Радищева д. № 33
7.4	Моноблок (MSI MS-A912) – 27 шт. Моноблок (ASUS ET2220I) – 13 шт.
7.5	
7.6	
7.7	Кабинет курсового и дипломного проектирования (КМ53/УК-707)г. Курск, ул. Карла Маркса, д. 53, Учебный корпус, Карла Маркса, д. 53, Стол - 5 шт. , стул - 5 шт.;
7.8	Информационные стенды по дипломному и курсовому проектированию - 4 шт.
7.9	
7.10	Компьютерный класс (КМ53/УК-1301): Курск, ул. Карла Маркса, д. 53, Учебный корпус, Карла Маркса, д. 53
7.11	Стол - 17 шт., кресло - 17 шт., интерактивная доска smartboard - 1 шт., проектор Epson– 1 шт.; Рабочая станция (Dell OptiPlex 3050, Монитор DELL P2419H 23.8") - 15 шт.
7.12	
7.13	
7.14	

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.