

Документ подписан простой электронной подписью
Информация о владельце:

ФИО: Худин Александр Николаевич

Должность: Ректор

Дата подписания: 05.02.2021 14:25:52

Уникальный программный ключ:

08303ad8de1c60b987361de7085acb509ac3da145141b561af0ee97e73a1941

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: 37.04.01 ПСИХОЛОГИЯ

Профиль подготовки: Консультативная психология

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	
Неделя	9,3			
Вид занятий	УП	РП	УП	РП
Лекции	10	10	10	10
Лабораторные	10	10	10	10
Итого ауд.	20	20	20	20
Контактная работа	20	20	20	20
Сам. работа	52	52	52	52
Итого	72	72	72	72

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

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Минобрнауки России от 23.09.2015 г. № № 1043 "Об утверждении ФГОС ВО по направлению подготовки 37.04.01 ПСИХОЛОГИЯ (уровень магистратуры)"

Рабочая программа дисциплины "Кибербезопасность" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 37.04.01 ПСИХОЛОГИЯ профиль Консультативная психология

Составитель(и):

© Курский государственный университет, 2019

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)

ПК-2: готовностью модифицировать, адаптировать существующие и создавать новые методы и методики научно-исследовательской и практической деятельности в определенной области психологии с использованием современных информационных технологий

Знать:

основные методы внедрения современных ИТ, применяемые в практической, научно-исследовательской и психологической деятельности

Уметь:

осуществлять модификацию, адаптацию и создание новых методик в профессиональной деятельности

Владеть:

способами внедрения современных информационно-коммуникационных новейших мультимедиа-технологий в определенные области психологии

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	2	0
1.4	Основы файловой системы Требования к системам защиты информации.	Ср	4	10	0
1.5	Лабораторная работа №2	Лаб	4	2	0
1.6	Общая характеристика сетей и протоколов передачи данных	Ср	4	10	0
1.7	Антивирусы и защита электронного документооборота от не санкционированного доступа	Ср	4	6	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	Общие требования к паролям симметричное и не симметричное шифрование	Лек	4	2	0
2.2	Лабораторная работа №3	Лаб	4	1	0

2.3	Хэш-функция и электронная подпись и протоколы электронных данных	Лек	4	2	0
2.4	Защищенные каналы данных облачные технологии и защищённый документооборот	Ср	4	14	0
2.5	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	Лек	4	2	0
3.2	Нормативно-правовые акты и стандарты по кибербезопасности	Лаб	4	2	0
3.3	Преступления в сфере информационных технологий	Ср	4	10	0
3.4	Рубежный контроль	Лаб	4	2	0
3.5	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 информационной безопасности от «23» апреля 2019 г. протоколом № 11, 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 «23» апреля 2019 г. 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

6.1.3. 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	Сердюк В. А. Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. Издательство: Издательский дом Высшей школы экономики, 2015- http://biblioclub.ru/index.php?page=book_red&id=440285&sr=1		
Э2	Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации / Ю.Н. Загинайлов . — М. Берлин : Директ-Медиа, 2015 . — 253 с. — ISBN 978-5-4475-3946-7 - http://biblioclub.ru/index.php?page=book&id=276557		

ЭЗ	Нестеров, С. А. Основы информационной безопасности / С.А. Нестеров .— Санкт-Петербург : Издательство Политехнического университета, 2014 .— 322 с. — ISBN 978-5-7422-4331-1- http://biblioclub.ru/index.php?page=book&id=363040
6.3.1 Перечень программного обеспечения	
7.3.1.1	Microsoft Windows XP Professional Open License: 47818817;
7.3.1.2	Microsoft Windows 7 Professional Open License: 47818817;
7.3.1.3	Microsoft Office Professional 2003 Open License:42226254;
7.3.1.4	Microsoft Office Standart 2007 Open License:43219389;
7.3.1.5	7-Zip Свободная лицензия GNU LGPL;
7.3.1.6	Adobe Acrobat Reader DC Бесплатное программное обеспечение;
7.3.1.7	Google Chrome Свободная лицензия BSD;
7.3.1.8	Hot Potatoes Бесплатное проприетарное программное обеспечение;
7.3.1.9	ProjectLibre Бесплатное программное обеспечение по лицензии Common Public Attribution
7.3.1.10	License Version 1.0.
6.3.2 Перечень информационных справочных систем	
7.3.2.1	http://195.93.165.10:2280 – Электронный каталог библиотеки КГУ
7.3.2.2	http://elibrary.ru – Научная электронная библиотека
7.3.2.3	http://uisrussia.msu.ru – Университетская информационная система «Россия».

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Учебная аудитория (Р33/ГК-77) для проведения занятий лекционного типа, занятий
7.2	семинарского типа, групповых и индивидуальных консультаций, текущего контроля и
7.3	промежуточной аттестации
7.4	305000, Курская область, г. Курск, ул. Радищева д. № 33
7.5	Парта – 48 шт.
7.6	Стул – 86 шт.
7.7	Компьютер рабочая станция CEL D336/mb/775/512Mb – 10 шт.
7.8	Подставка под цветы – 3 шт.
7.9	Жалюзи – 5 шт.
7.10	Доска – 2 шт.
7.11	Проектор Optoma DX211 – 1 шт.
7.12	Экран – 1 шт.
7.13	Lenovo B590 – 1 шт
7.14	Переносной Нетбук DELL Inspiron 1018– 1 шт.
7.15	Интерактивная доска Hitachi Starboard FX-82WL – 1 шт.
7.16	Демонстрационный стенд – 1 шт.
7.17	Видеозапись конкурсных уроков и внеурочных занятий
7.18	Комплект мультимедийных презентаций:
7.19	«Учитель года»; «Педагогический дебют»
7.20	«Классификация методов обучения»
7.21	«Активные и интерактивные методы обучения»
7.22	«Теоретико-методологические основы инновационной деятельности в образовании»
7.23	«Современный вуз как самообучающаяся организация»
7.24	«Студентоцентристский и компетентностный подходы в системе высшего образования»
7.25	«Риски в инновационной деятельности образовательной организации»
7.26	«Проектирование инновационной деятельности в высшей школе. Управление проектами»
7.27	Аудитории для самостоятельной работы (Р29/УК-303)и (Р33/ЛК-146)
7.28	305000, Курская область, г. Курск, ул. Радищева д. № 33
7.29	
7.30	
7.31	

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 лекционный 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.