Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Худин Александр Николаевич
Должность: Ректор
Дата подписания: 05.02.2021 15:34:30
Уникальный программный ключ:
08303ad8de1c60b987361de7085acb509ac3da143f415362ffaf0ee37e73fa19

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное образовательное учреждение высшего образования
"Курский государственный университет"

Кафедра компьютерных технологий и информатизации образования

УТВЕРЖДЕНО

протокол заседания
Ученого совета от 29.04.2019 г., №9

Рабочая программа дисциплины
Цифровые технологии защиты информации в профессиональной деятельности

Направление подготовки: 44.04.01 Педагогическое образование

Профиль подготовки: Информационно-коммуникационные технологии в образовании

Квалификация: магистр

Форма обучения: очная

Общая трудоемкость 3 ЗЕТ

Виды контроля в семестрах:
экзамен(ы) 2

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**2 (1.2)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
В том числе инт.	2	2	2	2
Итого ауд.	32	32	32	32
Контактная работа	32	32	32	32
Сам. работа	40	40	40	40
Часы на контроль	36	36	36	36
Итого	108	108	108	108

Курск 2019

Рабочая программа дисциплины Цифровые технологии защиты информации в профессиональной деятельности / сост. ; Курск. гос. ун-т. - Курск, 2019. - с.

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Минобрнауки России от 22.02.2018 г. № 126 "Об утверждении ФГОС ВО по направлению подготовки 44.04.01 Педагогическое образование (уровень магистратуры)"

Рабочая программа дисциплины "Цифровые технологии защиты информации в профессиональной деятельности" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 44.04.01 Педагогическое образование профиль

Составитель(и):

© Курский государственный университет, 2019

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	- формирование у обучаемых системы знаний, умений и навыков в области необходимых для построения и анализа безопасных информационных систем и технологий;
1.2	- знакомство со структурой коммерческой тайны предприятия и необходимости ее защиты;
1.3	- изучение характеристики основных угроз информационной безопасности предприятия;
1.4	- рассмотрение возможных каналов утечки информации и методы промышленного шпионажа;
1.5	- получение общих представлений о существующих правовых, организационных методах и технических средствах защиты информации от несанкционированного доступа и от повреждения.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.ДВ.02

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-4: Способен использовать индивидуальные креативные способности для самостоятельного решения исследовательских задач
Знать:
требования к использованию индивидуальных креативных способностей.
Уметь:
использовать индивидуальные креативные способности для самостоятельного решения исследовательских задач в области высшего и профессионального образования.
Владеть:
технологиями использования индивидуальных креативных способностей для самостоятельного решения исследовательских задач; способами внедрения творческих идей в практику решения исследовательских задач в области высшего и профессионального образования

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем	Вид занятий	Семестр / Курс	Часов	Интеракт.
	Раздел 1. Основные понятия и определения предмета защиты информации	Раздел			
1.1	Понятие защиты информации. Базовые свойства безопасности информации.	Лек	2	4	2
1.2	Санкционированный и несанкционированный доступ.	Лек	2	4	0
1.3	Понятие угрозы, уязвимости, риска.	Лек	2	4	0
1.4	Каналы реализации угроз.	Лек	2	4	0
1.5	Компьютерные вирусы	Ср	2	4	0
1.6	Основные принципы обеспечения информационной безопасности.	Ср	2	4	0
1.7	Меры обеспечения безопасности компьютерных систем.	Ср	2	1	0
1.8	Ценность информации.	Ср	2	1	0
1.9	Характеристика способов защиты компьютерной информации с помощью аппаратно-программных мер.	Ср	2	1	0
	Раздел 2. Идентификация и аутентификация субъектов	Раздел			
2.1	Понятие идентификации и аутентификации.	Лаб	2	6	0

2.2	Парольные системы идентификации и аутентификации пользователей	Ср	2	1	0
2.3	Количественная оценка стойкости парольной защиты	Лаб	2	6	0
2.4	Идентификация и аутентификация с использованием технических устройств.	Ср	2	2	0
2.5	Биометрическая аутентификация.	Ср	2	2	0
2.6	Защита информации	Ср	2	2	0
2.7	Контроль ввода в редакторе электронных таблиц	Ср	2	2	0
	Раздел 3. Разграничение доступа к ресурсам	Раздел			
3.1	Политики безопасности.	Лаб	2	2	0
3.2	Контроль конфиденциальности. Политики избирательного разграничения доступа.	Ср	2	4	0
3.3	Контроль конфиденциальности. Контроль доступа, базирующийся на ролях.	Ср	2	1	0
3.4	Контроль конфиденциальности. Мандатные политики безопасности.	Ср	2	1	0
3.5	Реализация политик информационной безопасности. дискреционная модель политики безопасности	Лаб	2	2	0
3.6	Мандатные модели политики безопасности.	Ср	2	4	0
3.7	Исследование стандартных защитных средств ОС Windows и пакета Microsoft Office	Ср	2	2	0
3.8	Управление пользователями и их правами доступа в ОС Windows	Ср	2	2	0
3.9	Принципы криптографической защиты информации.	Ср	2	2	0
3.10	Электронно-цифровая подпись.	Ср	2	4	0

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине «Современные компьютерные технологии и безопасность в сфере физической культуры» рассмотрены и одобрены на заседании кафедры компьютерных технологий и информатизации образования от «24» марта 2017 г. протокол № 8, являются приложением к рабочей программе.

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточной аттестации по дисциплине «Современные компьютерные технологии и безопасность в сфере физической культуры» рассмотрены и одобрены на заседании кафедры компьютерных технологий и информатизации образования от «24» марта 2017 г. протокол № 8, 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	Прохорова О. В. - Информационная безопасность и защита информации: Учебник - Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.	http://www.iprbookshop.ru/43183	1
Л1.2	Рытенкова О. - Информационная безопасность: журнал - Москва: ГРОТЕК, 2014.	http://biblioclub.ru/index.php?page=book&id=238445	1

6.1.2. Дополнительная литература

	Заглавие	Эл. адрес	Кол-

	Заглавие	Эл. адрес	Кол-
Л2.1	Артемов А. В. - Информационная безопасность: курс лекций - Орел: МАБИВ, 2014.	http://biblioclub.ru/index.php?page=book&id=428605	1

6.1.3. Методические разработки

	Заглавие	Эл. адрес	Кол-
Л3.1	Нестеров С. А. - Информационная безопасность: Учебник и практикум - М.: Издательство Юрайт, 2017.	http://www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7	1
Л3.2	Шаньгин В.Ф. - Информационная безопасность и защита информации: учебное пособие - Саратов: Профобразование, 2017.	http://www.iprbookshop.ru/63594.html	1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	1. Официальный сайт программы PDFCreator [Электронный ресурс]: — Режим доступа: http://pdfcreator.ru/ 2. Официальный сайт программы Protectorion ToGo [Электронный ресурс]: — Режим доступа: http://en.protectorion.com/ 3. Официальный сайт программы Recuva [Электронный ресурс]: — Режим доступа: http://www.piriform.com/recuva 4. Официальный сайт программы Handy Recovery [Электронный ресурс]: — Режим доступа: http://www.handyrecovery.ru/ 5. Официальный сайт программы Pandora Recovery [Электронный ресурс]: — Режим доступа: http://www.pandorarecovery.com/local/ru/ 6. Официальный сайт программы Dr.Web [Электронный ресурс]: — Режим доступа: http://www.drweb.ru/ 7. Официальный сайт компании «Консультант Плюс» [Электронный ресурс]: — Режим доступа: http://www.consultant.ru/

6.3.1 Перечень программного обеспечения

7.3.1.1	PDFCreator
7.3.1.2	Protectorion ToGo
7.3.1.3	Recuva
7.3.1.4	Handy Recovery
7.3.1.5	Pandora Recovery
7.3.1.6	Dr.Web
7.3.1.7	Windows
7.3.1.8	MS Office

6.3.2 Перечень информационных справочных систем

7.3.2.1	Электронная библиотечная система «Юрайт» - https://www.biblio-online.ru/
7.3.2.2	Электронная библиотечная система КГУ - http://library-reader.kursksu.ru/
7.3.2.3	Электронная библиотечная система «Университетская библиотека ONLINE» - http://biblioclub.ru/
7.3.2.4	Научная электронная библиотека - http://www.elibrary.ru
7.3.2.5	Российская государственная библиотека - http://www.rsl.ru
7.3.2.6	«Консультант Плюс» [Электронный ресурс]: — Режим доступа: http://www.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, укомплектована учебной мебелью, проектором, ноутбуком.
7.2	Компьютерная аудитория для проведения лабораторных и практических занятий, укомплектована:
7.3	-Комплекты учебных столов и стульев;
7.4	-Комплекты компьютерных столов и стульев;
7.5	-Интерактивная доска;
7.6	-Компьютеры;
7.7	-Мультимедийный проектор;
7.8	-Ноутбук.
7.9	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.
7.10	Наборы демонстрационного оборудования и учебно-наглядных пособий, представленных комплектом мультимедийных презентаций.

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

Методические рекомендации по организации самостоятельной
работы студентов

Самостоятельная работа студентов – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студента по усвоению учебного материала может выполняться в читальном зале библиотеки, учебных кабинетах (лабораториях), компьютерных классах, дома. Студент подбирает научную и специальную монографическую и периодическую литературу в соответствии с рекомендациями преподавателя или самостоятельно. При организации самостоятельной работы студентов с использованием технических средств, обеспечивающих доступ к информации (компьютерных баз данных, систем автоматизированного проектирования и т.п.), должно быть предусмотрено и получение необходимой консультации или помощи со стороны преподавателей.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию. Основными видами самостоятельной работы студентов с участием преподавателя являются:

- текущие консультации;
- прием и защита практических работ (во время проведения практических работ).

Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия. Основными видами самостоятельной работы студентов без участия преподавателей являются:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы;
- написание рефератов;
- подготовка к семинарам и практическим работам, их оформление;
- текущий контроль успеваемости на базе обучающих и аттестующих тестов.

Самостоятельная работа студентов требует наличия информационно-предметного обеспечения: учебников, учебных и методических пособий, конспектов лекций. Методические материалы должны обеспечивать возможность самоконтроля студента по блоку учебного материала или предмета в целом.

Важным фактором усвоения материала дисциплины и является самостоятельная работа студентов. Эта работа состоит из непрерывной работы по выполнению текущих заданий, циклической работы по выполнению рефератов по целым разделам (темам) дисциплины. Результативность самостоятельной работы студентов обеспечивается эффективной системой контроля.

Примерная тематика учебно-исследовательских заданий

1. «Владелец сертификата ключа подписи» в соответствии с Федеральным законом от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи"
2. Определение термина «коммерческая тайна» на основе Федерального закона «О коммерческой тайне» и ст. 139 ГК РФ. Группы баз данных отнесенные к коммерческой тайне.
3. Основные понятия, используемые в Федеральном законе от 27.07.2006 г . № 149-ФЗ «Об информации, информационных технологиях и защите информации» (далее ФЗ «Об информации»).
4. Ограничение доступа к информации на основании ст. 9 ФЗ «Об информации».
5. Специальные категории персональных баз данных в соответствии с ФЗ «О персональных данных».
6. Дать определение терминам «Аналоговые данные», «Аналоговый документ; АнД (аналоговая форма документа)», в соответствии с ГОСТ Р 52292-2004. Информационная технология. Электронный обмен информацией. Термины и определения.
7. Дать определение «данные» в соответствии с ГОСТ Р 52292-2004. Информационная технология. Электронный обмен информацией.
8. Дать определения терминов «Администратор автоматизированной системы (администратор АС)», «Администратор защиты», «Администратор базы данных». Различие и единство данных терминов.
9. Назовите основные направления мер защиты информации на основании ст.16. ФЗ «Об информации».
10. Права субъекта персональных данных – физического лица в соответствии с ФЗ «О Персональных данных»
11. Жизненный цикл автоматизированной системы (АС) в соответствии с ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы.
12. Дать определение терминов «Аутентичный документ», «Атрибут», в соответствии с ГОСТ 2.051-2006. Единая система конструкторской документации. Электронные документы. Общие положения
13. Идентичность данных в соответствии с ГОСТ Р 51170-98. Качество служебной информации.
14. Кодекс Российской Федерации об административных правонарушениях (КоАП РФ) в области правил защиты информации (ст. 13.11, 13.12, 13.13, 13.14, 17.13).
15. Уголовный кодекс РФ (УК РФ) о компьютерных преступлениях (ст.272)
16. УК РФ о компьютерных преступлениях (ст. 273)
17. УК РФ о компьютерных преступлениях (ст.274)
18. УК РФ о преступлениях, связанных с получением и разглашением информации, составляющей коммерческую, налоговую или банковскую тайну