МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. УТКИНА»

Кафедра «Государственного, муниципального и корпоративного управления»

«СОГЛАСОВАНО»
Директор ИМА
_____ Бодров О.А.
«26» 06 2020 г.

Заведующий кафедрой
_____ Перфильев С.В.
«26» 06 2020 г.

«УТВЕРЖДАЮ»
Проректор по РОПиМД
_____ Корячко А.В.
«26» 06 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.12 «Информационная безопасность»

Направление подготовки
38.04.04 «Государственное и муниципальное управление»

Профиль – Информационные технологии в государственном и муниципальном управлении

ОПОП академической магистратуры
«Государственное и муниципальное управление»

Формы обучения – очно-заочная

Рязань, 2020

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования по направлению подготовки (специальности) Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.04.04 «Государственное и муниципальное управление», утвержденным приказом Минобрнауки России № 1518 от 26.11.2014 г.

Разработчик

доцент кафедры АСУ / Челебаев С. В. /

(должность, кафедра) (подпись) (Расшифровка)

Заведующий кафедрой

АСУ / Холонов С. Ч. /

(кафедра) (подпись) (Расшифровка)

Рассмотрена и утверждена на заседании кафедры « 25 » июня 2020 г., протокол № 10

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Программа по дисциплине «Информационная безопасность» составлена с требованиями, установленными Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.04.04 Государственное и муниципальное управление (уровень магистратуры), утвержденным Приказом Минобрнауки России № 1518 от 26.11.2014 г. (с изм. и доп.).

Программа предназначена для студентов, обучающихся по основной профессиональной образовательной программе высшего образования (далее - ОПОП ВО) «Информационные технологии в государственном и муниципальном управлении», реализуемой в рамках направления подготовки 38.04.04 Государственное и муниципальное управление (уровень магистратуры).

Целью освоения дисциплины «Информационная безопасность» является ознакомление обучающихся с основными направлениями деятельности по обеспечению информационной безопасности, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей, и методов их применения.

Задачи освоения учебной дисциплины:

- сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния;
- передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;
- сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

Перечень планируемых результатов обучения по дисциплине

Коды компе-тенций	***Результаты освоения ООП Содержание компетенций***	***Перечень планируемых результатов обучения при прохождении практики***
ПК-11	способностью осуществлять верификацию и структуризацию информации, получаемой из разных источников	Знать: понятия информационной безопасности, основные составляющие информационной безопасности. Уметь: выбрать соответствующие информационные технологии обеспечения информационной безопасности. Владеть: навыками использования технологий информационной безопасности

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Правовое обеспечение государственного и муниципального управления» реализуется в рамках базовой части Блока 1 учебного плана ОПОП. Дисциплина изучается на 2 курсе в 3 семестре.

Для освоения дисциплины необходимы компетенции правового содержания, сформированные в результате прохождения программ бакалавриата.

Знания, полученные в ходе изучения дисциплины «Информационная безопасность» логически связаны с дисциплинами, изучаемыми студентами параллельно, например: «Информационно-аналитические технологии в государственном и муниципальном управлении».

Материал дисциплины формирует экономические и организационные основы для НИР, практик и выпускной квалификационной работы.

3. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость (объем) дисциплины составляет 3 зачетные единицы (з.е.), 108 часа.

Вид учебной работы	**Всего часов**
Общая трудоемкость дисциплины, в том числе:	108
1. Контактная работа обучающихся с преподавателем (всего), в том числе:	42,35
лекции	8
практические занятия	32
консультации	2
иные виды контактной работы	0,35
2. Самостоятельная работа обучающихся (всего), в том числе:	12
курсовой проект (работа)	-
самостоятельные занятия	12
3. Контроль	53,65
Вид промежуточной аттестации обучающихся	экзамен

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Разделы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах)

Раздел дисциплины	Общая трудоемкость	Контактная работа			Самостоятельная работа
		Всего	Лекции	ПЗ	
Понятие информационной безопасности. Основные составляющие	6	5	1	4	1
Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и её составляющие	6	5	1	4	1
Законодательный уровень информационной безопасности. Административный уровень информационной безопасности	6	5	1	4	1
Процедурный уровень информационной безопасности	6	5	1	4	1
Основные характеристики программно-технических мер. Идентификация и аутентификация	7	5	1	4	2
Протоколирование и аудит, шифрование, контроль целостности.	7	5	1	4	2

Экранирование, анализ защищенности	7	5	1	4	2
Обеспечение высокой доступности	7	5	1	4	2
Консультации	2	2			
ИКР	0,35	0,35			
Контроль	53,65				
Всего	108	42,35	8	32	12

Содержание дисциплины

Лекционные занятия

№	Наименование раздела дисциплины	Содержание раздела
1	Понятие информационной безопасности. Основные составляющие	Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем.
2	Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и её составляющие	Сложные системы. Структурный подход. Объектно-ориентированный подход, класс, объект, метод объекта, инкапсуляция, наследование, полиморфизм, грань объекта, уровень детализации ИС, деление на субъекты и объекты, безопасность повторного использования объектов, учет семантики. Операционная система как сервис безопасности. Основные определения и критерии классификации угроз. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.
3	Законодательный уровень информационной безопасности. Административный уровень информационной безопасности	Российское законодательство в области информационной безопасности. Зарубежное законодательство в области информационной безопасности. Стандарты и спецификации в области информационной безопасности. Основные понятия административного уровня, политика безопасности. Жизненный цикл информационной системы. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками
4	Процедурный уровень информационной безопасности	Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.
5	Основные характеристики программно-технических мер. Идентификация и аутентификация	Основные понятия программно-технического уровня. Архитектурная безопасность. Экранирование. Анализ защищённости. Отказоустойчивость. Безопасное восстановление. Основные понятия. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации

		Kerberos. Идентификация/аутентификация с помощью биометрических данных. Управление доступом. Ролевое управление доступом.
6	Протоколирование и аудит, шифрование, контроль целостности	Основные понятия. Активный аудит. Шифрование. Симметричный метод шифрования. Асимметричный метод шифрования. Секретный и открытый ключ. Криптография. Контроль целостности. Цифровые сертификаты. Электронная цифровая подпись.
7	Экранирование, анализ защищенности	Основные понятия. Экранирование. Фильтрация. Межсетевые экраны. Классификация межсетевых экранов. Архитектурная безопасность. Транспортное экранирование. Анализ защищенности. База данных уязвимостей. Сетевой сканер. Антивирусная защита.
8	Обеспечение высокой доступности	Эффективность услуг. Время недоступности. Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Обеспечение обслуживаемости. Туннелирование.

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Фомин Д.В. Информационная безопасность [Электронный ресурс]: учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения/ Фомин Д.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 54 c.— Режим доступа: http://www.iprbookshop.ru/77320.html.— ЭБС «IPRbooks»

2. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 c.— Режим доступа: http://www.iprbookshop.ru/33430.html.— ЭБС «IPRbooks»

3. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 154 c.— Режим доступа: http://www.iprbookshop.ru/52160.html.— ЭБС «IPRbooks»

6. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы приведены в приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «Информационная безопасность»).

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

а) основная учебная литература:

1. Фомин Д.В. Информационная безопасность [Электронный ресурс]: учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения/ Фомин Д.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 54 c.— Режим доступа: http://www.iprbookshop.ru/77320.html.— ЭБС «IPRbooks»

2. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 c.— Режим доступа: http://www.iprbookshop.ru/33430.html.— ЭБС «IPRbooks»

3. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 154 c.— Режим доступа: http://www.iprbookshop.ru/52160.html.— ЭБС «IPRbooks»

4. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 c.— Режим доступа: http://www.iprbookshop.ru/52209.html.— ЭБС «IPRbooks»

5. Авдошин С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс]/ Авдошин С.М., Савельева А.А., Сердюк В.А.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.— 412 c.— Режим доступа: http://www.iprbookshop.ru/72341.html.— ЭБС «IPRbooks»

6. Дождиков В.Г. Краткий энциклопедический словарь по информационной безопасности [Электронный ресурс]/ Дождиков В.Г., Салтан М.И.— Электрон. текстовые данные.— М.: Энергия, 2010.— 239 c.— Режим доступа: http://www.iprbookshop.ru/5729.html.— ЭБС «IPRbooks»

7. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 c.— Режим доступа: http://www.iprbookshop.ru/10677.html.— ЭБС «IPRbooks»

8. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: учебное пособие / Спицын В.Г.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011.— 148 c.— Режим доступа: http://www.iprbookshop.ru/13936.html.— ЭБС «IPRbooks»

9. Ю.И. Малинин, С.В. Аникеев, Д.Ю. Малинин Информационная безопасность и защита информации: метод. указ. к лаб. работам / РГРТА. Сост.: Ю.И. Малинин, С.В. Аникеев, Д.Ю. Малинин. Рязань, 2005. 32 с.

10. Ю.И.Малинин Информационная безопасность и защита информации: методические указания к лабораторным работам / РГРТУ. Сост. Ю.И.Малинин.- Рязань, 2009.- 24 с.

11. Ю.И.Малинин Информационная безопасность и защита информации: методические указания к лабораторным работам / РГРТУ. Сост. Ю.И.Малинин.- Рязань, 2011.- 24 с.

б) дополнительная учебная литература:

12. Федин Ф.О. Информационная безопасность [Электронный ресурс]: учебное пособие / Федин Ф.О., Офицеров В.П., Федин Ф.Ф.— Электрон. текстовые данные.— М.: Московский городской педагогический университет, 2011. — 260 c.— Режим доступа: http://www.iprbookshop.ru/26486.html.— ЭБС «IPRbooks»

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО–ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Ресурсы информационно-телекоммуникационной сети «интернет». Обучающимся предоставлена возможность индивидуального доступа к следующим электронно-библиотечным системам.

1. Электронно-библиотечная система «Лань», режим доступа – с любого компьютера РГРТУ без пароля. – URL: https://e.lanbook.com/

2. Электронно-библиотечная система «IPRbooks», режим доступа – с любого компьютера РГРТУ без пароля, из сети интернет по паролю. – URL: https://iprbookshop.ru/.

3. Электронная библиотека ЮРАЙТ, режим доступа из сети интернет без пароля. – URL: https://biblio-online.ru/info/free-books/.

4. Электронный ресурс «Виртуальная кафедра АСУ» – https://rgrty.ru/.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методически изучение дисциплины производится с применением активных форм проведения занятий. Принятая технология активного обучения базируется на работе, когда в процессе лекций и практических занятий, дополняемых самостоятельной работой обучаемых, выполняется серия проектно-исследовательских заданий и экспериментов, решение которых студентами позволяет практически применить полученные знания, развить необходимые компетенции по данной дисциплине.

Успешное освоение дисциплины во многом зависит от самостоятельной работы студента. Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

Изучение конспекта лекции в тот же день, после лекции – 10-15 минут.

Изучение теоретического материала по учебнику и конспекту – 1 час в неделю в ходе подготовки к лабораторной работе.

Кроме чтения учебной литературы из обязательного списка рекомендуется активно использовать информационные ресурсы сети Интернет по изучаемой теме. Ответы на многие вопросы, связанные с темами дисциплины Вы можете получить в сети Интернет, посещая соответствующие информационные ресурсы.

Самостоятельное изучение тем учебной дисциплины способствует:

- закреплению знаний, умений и навыков, полученных в ходе аудиторных занятий;
- углублению и расширению знаний по отдельным вопросам и темам дисциплины;
- освоению умений прикладного и практического использования полученных знаний в области информационной безопасности.

Самостоятельная работа как вид учебной работы может использоваться на лекциях и лабораторных работах, а также иметь самостоятельное значение – внеаудиторная самостоятельная работа обучающихся – при подготовке к лекциям, практическим занятиям, к экзамену.

Основными видами самостоятельной работы по дисциплине являются:

- самостоятельное изучение отдельных вопросов и тем дисциплины «Информационная безопасность»;
- выполнение лабораторного задания;
- оформление отчета по результатам лабораторных работ, подготовка к зачету.

Экзамен показывает степень освоения дисциплины обучающимся.

При подготовке к экзамену необходимо тщательно изучить лекционный материал, просмотреть все отчеты по лабораторным работам, чтобы еще раз осмыслить необходимость теории в практических задачах. Целесообразно после изучения (по лекционному материалу и другим информационным источникам) конкретного вопроса из числа контрольных вопросов к зачету попытаться по памяти записать ответ на бумаге в возможно более развернутом виде. Это способствует развитию зрительной памяти и даст студенту больше уверенности в том, что он усвоит материал. Возникшие в ходе подготовки вопросы, на которые студент не смог найти ответа, необходимо записать и выяснить их на консультации у преподавателя.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ),

ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННО-СПРАВОЧНЫХ СИСТЕМ

При проведении занятий по дисциплине используются следующие информационные технологии:

– удаленные информационные коммуникации между студентами и преподавателем, ведущим лекционные и практические занятия, посредством электронной почты, позволяющие осуществлять оперативный контроль графика выполнения и содержания контрольных заданий, решение организационных вопросов, удаленное консультирование;

– поиск актуальной научной, статистической и общественно-политической информации для выполнения самостоятельной работы и контрольных заданий;

– доступ к современным профессиональным базам данных и информационным справочным системам;

– выполнение студентами заданий с использованием лицензионного и свободно распространяемого программного обеспечения, установленного на рабочих местах студента в компьютерных классах и в помещениях для самостоятельной работы, а также для выполнения самостоятельной работы в домашних условиях.

Перечень лицензионного программного обеспечения:

– операционная система Windows;
– Kaspersky Endpoint Security;
– LibreOffice, лицензия LGPLv3

Перечень профессиональных баз данных (в том числе международным реферативным базам данных научных изданий) и информационных справочных систем:

– Информационно-правовой портал ГАРАНТ.РУ [Электронный ресурс]. – URL: http://www.garant.ru. – Режим доступа: свободный доступ.

– Справочная правовая система КонсультантПлюс [Электронный ресурс]. – URL: http://www.consultant.ru/online/. – Режим доступа: свободный доступ (будние дни – 20.00-24.00, выходные и праздничные дни – круглосуточно).

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, № 254 главного учебного корпуса	1 проектор NEC NP 216 G, 1 экран, 1 компьютер Pentium G 620, маркерная доска, 32 ученических стола, 64 места Экран с ручным приводом – 1 шт. Доска маркерная 120х200 см Подключение к сети «Интернет» и обеспечение доступа в электронную информационно-образовательную среду РГРТУ.
Учебно-административный корпус, а.424б Помещение для самостоятельной работы	11 посадочных мест, компьютерная техника (8ПК - ПЭВМ Pentium 733, ПЭВМ G620, Ноутбук HP dv8-1250er, Офисный ПК Samsung, ПЭВМ

	"Pentium-4", ПЭВМ № 2, Ноутбук DEXP, Компьютер) с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду РГРТУ, специализированная мебель (стулья-11, столы-11)

ПРИЛОЖЕНИЕ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. УТКИНА»

Кафедра «Государственного, муниципального и корпоративного управления»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Б1.В.12 «Информационная безопасность»

Направление подготовки
38.04.04 «Государственное и муниципальное управление»

Профиль – Информационные технологии в государственном и муниципальном управлении

ОПОП академической магистратуры
«Государственное и муниципальное управление»

Формы обучения – очно-заочная

Рязань, 2020

1. ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы - это совокупность учебно-методических материалов (контрольных заданий, описаний форм и процедур), предназначенных для оценки качества освоения обучающимися данной дисциплины как части ОПОП ВО.

Цель - оценить соответствие знаний, умений и уровня приобретенной компетенции обучающихся целям и требованиям основной образовательной программы в ходе проведения промежуточной аттестации.

Основная задача - обеспечить оценку уровня сформированности общекультурной компетенции, приобретаемой обучающимся в соответствии с этими требованиями.

Промежуточная аттестация – экзамен.

2. ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ

Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции (или её части)	Наименование оценочного средства
Понятие информационной безопасности. Основные составляющие	ПК-11	Экзамен
Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и её составляющие	ПК-11	Экзамен
Законодательный уровень информационной безопасности. Административный уровень информационной безопасности	ПК-11	Экзамен
Процедурный уровень информационной безопасности	ПК-11	Экзамен
Основные характеристики программно-технических мер. Идентификация и аутентификация	ПК-11	Экзамен
Протоколирование и аудит, шифрование, контроль целостности.	ПК-11	Экзамен
Экранирование, анализ защищенности	ПК-11	Экзамен
Обеспечение высокой доступности	ПК-11	Экзамен

3. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Итоговая оценка по дисциплине выставляется по шкале «неудовлетворительно», «удовлетворительно», «хорошо» и «отлично».

Критерии оценивания компетенций (результатов)

1. Уровень усвоения материала, предусмотренного программой.
2. Умение анализировать материал, устанавливать причинно-следственные связи.
3. Качество ответов на вопросы: логичность, убежденность, общая эрудиция.
4. Использование дополнительной литературы при подготовке ответов.
5. Умение вести поиск необходимой информации в сети Интернет.
6. Инициативность, умение работать в коллективе.
7. Качество оформления отчетной документации.

Примеры контрольных вопросов

1. Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб.

2. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем.

3. Сложные системы. Структурный подход.

4. Основные определения и критерии классификации угроз.

5. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник.

6. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.

7. Российское законодательство в области информационной безопасности.

8. Зарубежное законодательство в области информационной безопасности.

9. Стандарты и спецификации в области информационной безопасности.

10. Основные понятия, политика безопасности.

11. Жизненный цикл информационной системы.

12. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками.

13. Основные классы мер процедурного уровня.

14. Управление персоналом. Физическая защита.

15. Поддержание работоспособности.

16. Реагирование на нарушения режима безопасности.

17. Планирование восстановительных работ.

18. Основные понятия программно-технического уровня. Архитектурная безопасность.

19. Экранирование. Анализ защищённости.

20. Отказоустойчивость. Безопасное восстановление.

21. Основные понятия криптографии.

22. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации Kerberos.

23. Идентификация/аутентификация с помощью биометрических данных.

24. Управление доступом. Ролевое управление доступом.

25. Активный аудит. Шифрование.

26. Симметричный метод шифрования.

27. Асимметричный метод шифрования.

28. Секретный и открытый ключ.

29. Криптография. Контроль целостности

30. Цифровые сертификаты.

31. Электронная цифровая подпись.

32. Экранирование. Фильтрация. Межсетевые экраны.

33. Классификация межсетевых экранов.

34. Архитектурная безопасность.

35. Транспортное экранирование. Анализ защищенности.

36. Сетевой сканер. Антивирусная защита.

Формы текущего контроля

Текущий контроль по дисциплине проводится в виде тестовых опросов по отдельным темам дисциплины, проверки заданий, выполняемых на практических занятиях.

Формы промежуточного контроля

Промежуточный контроль по дисциплине – отчет о выполнении практического.

Формы заключительного контроля

Форма заключительного контроля по дисциплине – экзамен.

Критерий допуска к экзамену

К экзамену допускаются студенты, выполнившие ко дню проведения экзамена все практические задания.