МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

СОГЛАСОВАНО
Зав. выпускающей кафедры

УТВЕРЖДАЮ

Информационная безопасность

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Государственного, муниципального и корпоративного управления**

Учебный план v38.04.04_25_00.plx
38.04.04 Государственное и муниципальное управление

Квалификация **магистр**

Форма обучения **очно-заочная**

Общая трудоемкость **3 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		Итого	
Недель	8			
Вид занятий	УП	РП	УП	РП
Лекции	8	8	8	8
Практические	16	16	16	16
Иная контактная работа	0,35	0,35	0,35	0,35
Консультирование перед экзаменом и практикой	2	2	2	2
Итого ауд.	26,35	26,35	26,35	26,35
Контактная работа	26,35	26,35	26,35	26,35
Сам. работа	46	46	46	46
Часы на контроль	35,65	35,65	35,65	35,65
Итого	108	108	108	108

г. Рязань

Программу составил(и):
к.т.н., доц., Челебаев С.В.

Рабочая программа дисциплины
Информационная безопасность

разработана в соответствии с ФГОС ВО:
ФГОС ВО - магистратура по направлению подготовки 38.04.04 Государственное и муниципальное управление (приказ Минобрнауки России от 13.08.2020 г. № 1000)

составлена на основании учебного плана:
38.04.04 Государственное и муниципальное управление
утвержденного учёным советом вуза от 28.02.2025 протокол № 8.

Рабочая программа одобрена на заседании кафедры
Государственного, муниципального и корпоративного управления

Протокол от 04.04.2025 г. № 4
Срок действия программы: 2025-2028 уч.г.
Зав. кафедрой Перфильев Сергей Валерьевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
Государственного, муниципального и корпоративного управления

Протокол от __ _____ 2026 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
Государственного, муниципального и корпоративного управления

Протокол от __ _____ 2027 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры
Государственного, муниципального и корпоративного управления

Протокол от __ _____ 2028 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2029-2030 учебном году на заседании кафедры

Государственного, муниципального и корпоративного управления

Протокол от __ _____ 2029 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	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.
1.2	Задачи дисциплины:
1.3	- сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния;
1.4	- передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;
1.5	- сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Социальное проектирование
2.1.2	Управление территориальным развитием
2.1.3	Антикоррупционная политика
2.1.4	Ознакомительная практика
2.1.5	Проектный офис
2.1.6	Учебная практика
2.1.7	Государственная тарифная политика
2.1.8	Политический менеджмент и электронная демократия
2.1.9	Теория и механизмы современного государственного управления
2.1.10	Управление в социальной сфере
2.1.11	Управление в социальной сфере
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.2	Преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-2: Способен разрабатывать и реализовывать проекты в сфере государственного и муниципального управления
ПК-2.3. Принимает управленческие решения с учетом требований защиты персональной и личной информации
Знать **Уметь** **Владеть**

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	основные понятия информационной безопасности; распространенные угрозы информационной безопасности; требования защиты персональной и личной информации
3.2	**Уметь:**
3.2.1	принимать управленческие решения с учетом требований защиты персональной и личной информации
3.3	**Владеть:**
3.3.1	методами принятия управленческих решений на законодательном, административном и процедурном уровнях информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Форма контроля**

	Раздел 1. Понятие информационной безопасности, ее основные составляющие					
1.1	Понятие информационной безопасности, ее основные составляющие /Тема/	4	0			
1.2	Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем /Лек/	4	1		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
1.3	Понятие информационной безопасности, ее основные составляющие /Ср/	4	4		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
	Раздел 2. Объектно-ориентированный подход к рассмотрению защищаемых систем					
2.1	Объектно-ориентированный подход к рассмотрению защищаемых систем /Тема/	4	0			
2.2	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 /Лек/	4	1		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
2.3	Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и её составляющие /Ср/	4	4		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
	Раздел 3. Законодательный уровень информационной безопасности. Административный уровень информационной безопасности					
3.1	Законодательный уровень информационной безопасности. Административный уровень информационной безопасности /Тема/	4	0			
3.2	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 /Лек/	4	1		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен

3.3	Законодательный уровень информационной безопасности. Административный уровень информационной безопасности /Ср/	4	4		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
	Раздел 4. Процедурный уровень информационной безопасности					
4.1	Процедурный уровень информационной безопасности /Тема/	4	0			
4.2	Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ /Лек/	4	1		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
4.3	Процедурный уровень информационной безопасности /Ср/	4	4		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
	Раздел 5. Основные характеристики программно-технических мер. Идентификация и аутентификация					
5.1	Основные характеристики программно-технических мер. Идентификация и аутентификация /Тема/	4	0			
5.2	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 /Лек/	4	1		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
5.3	Идентификация и аутентификация /Пр/	4	4		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Отчет о выполнении практической работы
5.4	Основные характеристики программно-технических мер. Идентификация и аутентификация /Ср/	4	6		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
	Раздел 6. Протоколирование и аудит, шифрование, контроль целостности					
6.1	Протоколирование и аудит, шифрование, контроль целостности /Тема/	4	0			

6.2	Основные понятия. Активный аудит. Шифрование. Симметричный метод шифрования. Асимметричный метод шифрования. Секретный и открытый ключ. Криптография. Контроль целостности. Цифровые сертификаты. Электронная цифровая подпись /Лек/	4	1		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
6.3	Шифрование /Пр/	4	4		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Отчет о выполнении практической работы
6.4	Криптография /Пр/	4	4		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Отчет о выполнении практической работы
6.5	Протоколирование и аудит, шифрование, контроль целостности /Ср/	4	8		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
	Раздел 7. Экранирование, анализ защищенности. Обеспечение высокой доступности					
7.1	Экранирование, анализ защищенности. Обеспечение высокой доступности /Тема/	4	0			
7.2	Основные понятия. Экранирование. Фильтрация. Межсетевые экраны. Классификация межсетевых экранов. Архитектурная безопасность. Транспортное экранирование. Анализ защищенности. База данных уязвимостей. Сетевой сканер. Антивирусная защита /Лек/	4	1		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
7.3	Экранирование /Пр/	4	4		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Отчет о выполнении практической работы
7.4	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 /Ср/	4	8		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
	Раздел 8. Обеспечение высокой доступности					
8.1	Обеспечение высокой доступности /Тема/	4	0			
8.2	Эффективность услуг. Время недоступности. Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Обеспечение обслуживаемости. Туннелирование /Лек/	4	1		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен

8.3	Обеспечение высокой доступности /Ср/	4	8		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Контрольные вопросы, экзамен
	Раздел 9. Промежуточная аттестация					
9.1	Подготовка к зачету, иная контактная работа /Тема/	4	0			
9.2	Подготовка к экзамену /Экзамен/	4	35,65		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Экзамен
9.3	Консультация /Кнс/	4	2		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Экзамен
9.4	Прием экзамена /ИКР/	4	0,35		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4	Экзамен

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные средства по дисциплине "Информационная безопасность" представлены в приложении к рабочей программе дисциплины

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.1	Башлы П. Н., Бабаш А. В., Баранова Е. К.	Информационная безопасность и защита информации : учебное пособие	Москва: Евразийский открытый институт, 2012, 311 с.	978-5-374-00301-7, http://www.iprbookshop.ru/10677.html
Л1.2	Федин Ф. О., Офицеров В. П., Федин Ф. Ф.	Информационная безопасность : учебное пособие	Москва: Московский городской педагогический университет, 2011, 260 с.	2227-8397, http://www.iprbookshop.ru/26486.html
Л1.3	Артемов А. В.	Информационная безопасность : курс лекций	Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014, 256 с.	2227-8397, http://www.iprbookshop.ru/33430.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.4	Петров С. В., Кисляков П. А.	Информационная безопасность : учебное пособие	Саратов: Ай Пи Ар Букс, 2015, 326 с.	978-5-906-17271-6, http://www.iprbookshop.ru/33857.html
6.1.2. Дополнительная литература				
№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Прохорова О. В.	Информационная безопасность и защита информации : учебник	Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014, 113 с.	978-5-9585-0603-3, http://www.iprbookshop.ru/43183.html
Л2.2	Омарова С. А., Искакова К. А., Тойганбаева Н. А.	Информационная безопасность и защита информации : учебно-методический комплекс	Алматы: Нур-Принт, 2012, 98 с.	9965-756-05-8, http://www.iprbookshop.ru/67055.html
Л2.3	Горюхина Е. Ю., Литвинова Л. И., Ткачева Н. В.	Информационная безопасность : учебное пособие	Воронеж: Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015, 221 с.	2227-8397, http://www.iprbookshop.ru/72672.html
6.1.3. Методические разработки				
№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.1	Смышляев А. Г.	Информационная безопасность. Лабораторный практикум : учебное пособие	Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2015, 102 с.	2227-8397, http://www.iprbookshop.ru/66655.html
Л3.2	Малинин Ю.И., Аникеев С.В., Малинин Д.Ю.	Информационная безопасность и защита информации : Методические указания	Рязань: РИЦ РГРТУ, 2005,	, https://elib.rsreu.ru/ebs/download/302
Л3.3	Малинин Ю.И.	Информационная безопасность и защита информации : Методические указания	Рязань: РИЦ РГРТУ, 2009,	, https://elib.rsreu.ru/ebs/download/851
Л3.4	Малинин Ю.И.	Информационная безопасность и защита информации : Методические указания	Рязань: РИЦ РГРТУ, 2011,	, https://elib.rsreu.ru/ebs/download/1640

6.3 Перечень программного обеспечения и информационных справочных систем

6.3.1 Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование	Описание
Visual studio community	Свободное ПО
LibreOffice	Свободное ПО

6.3.2 Перечень информационных справочных систем

6.3.2.1	Система КонсультантПлюс http://www.consultant.ru

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1	254 учебно-административный корпус . Учебная аудитория кафедры АСУ для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 64 места, 1 проектор, 1 экран, 1 компьютер, специализированная мебель, маркерная доска
2	118 учебно-административный корпус. Учебная аудитория для проведения практических занятий, лабораторных работ 21 ПК Intel Pentium CPU G620, 2.6GHz, 4Gb ОЗУ, HDD 500Gb
3	127 учебно-административный корпус. Учебная аудитория для проведения практических занятий, лабораторных работ 25 ПК Intel Pentium CPU G620, 2.6GHz, 4Gb ОЗУ, HDD 500Gb

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Методические указания по освоению дисциплины "Информационная безопасность" представлены в приложении к рабочей программе дисциплины