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 **Автоматизированных систем управления**

Учебный план 38.03.04_24_00.plx
38.03.04 Государственное и муниципальное управление

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **2 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	8			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Иная контактная работа	0,25	0,25	0,25	0,25
Итого ауд.	32,25	32,25	32,25	32,25
Контактная работа	32,25	32,25	32,25	32,25
Сам. работа	31	31	31	31
Часы на контроль	8,75	8,75	8,75	8,75
Итого	72	72	72	72

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 - бакалавриат по направлению подготовки 38.03.04 Государственное и муниципальное управление (приказ Минобрнауки России от 13.08.2020 г. № 1016)

составлена на основании учебного плана:
38.03.04 Государственное и муниципальное управление
утвержденного учёным советом вуза от 26.01.2024 протокол № 8.

Рабочая программа одобрена на заседании кафедры
Автоматизированных систем управления

Протокол от 24.04.2024 г. № 11
Срок действия программы: 2024-2028 уч.г.
Зав. кафедрой Холопов Сергей Иванович

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Автоматизированных систем управления

Протокол от __ _____ 2025 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
Автоматизированных систем 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
Автоматизированных систем 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

Автоматизированных систем управления

Протокол от __ _____ 2028 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	Требования к входным знаниям, умениям и компетенциям студента, необходимые для изучения данной дисциплины, совпадают с выходными знаниями, умениями и компетенциями, полученными в ходе изучения следующих дисциплин предусмотренных учебным планом подготовки бакалавров: «Информационно-коммуникационные технологии в профессиональной сфере», «Web-программирование».
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
2.2.3	Производственная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-2: Способен применять знания основ информационной безопасности, основные положения законодательства о персональных данных, электронной подписи

ПК-2.1. Применяет знания основ информационной безопасности

Знать
понятие информационной безопасности и ее основные составляющие; объектно-ориентированный подход к рассмотрению защищаемых систем; основные классы мер процедурного уровня информационной безопасности; основные понятия программно-технического уровня информационной безопасности
Уметь
применять объектно-ориентированный подход к рассмотрению защищаемых систем; применять основные классы мер процедурного уровня информационной безопасности; применять основные понятия программно-технического уровня информационной безопасности
Владеть
основными подходами к рассмотрению защищаемых систем; классами мер процедурного уровня информационной безопасности; методами программно-технического уровня информационной безопасности

ПК-2.2. Применяет основные положения законодательства о персональных данных, электронной подписи

Знать
российское законодательство в области информационной безопасности; основные положения о цифровых сертификатах и электронной цифровой подписи; основы экранирования; основы мер обеспечения высокой доступности
Уметь
применять основные положения российского законодательства в области информационной безопасности; применять основные положения о цифровых сертификатах и электронной цифровой подписи; применять экранирование; применять меры обеспечения высокой доступности
Владеть
основными положениями о цифровых сертификатах и электронной цифровой подписи

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**

3.1.1	понятие информационной безопасности и ее основные составляющие; объектно-ориентированный подход к рассмотрению защищаемых систем; основные классы мер процедурного уровня информационной безопасности; основные понятия программно-технического уровня информационной безопасности; российское законодательство в области информационной безопасности; основные положения о цифровых сертификатах и электронной цифровой подписи; основы экранирования; основы мер обеспечения высокой доступности
3.2	**Уметь:**
3.2.1	применять объектно-ориентированный подход к рассмотрению защищаемых систем; применять основные классы мер процедурного уровня информационной безопасности; применять основные понятия программно-технического уровня информационной безопасности; применять основные положения российского законодательства в области информационной безопасности; применять основные положения о цифровых сертификатах и электронной цифровой подписи; применять экранирование; применять меры обеспечения высокой доступности
3.3	**Владеть:**
3.3.1	основными подходами к рассмотрению защищаемых систем; классами мер процедурного уровня информационной безопасности; методами программно-технического уровня информационной безопасности; основными положениями о цифровых сертификатах и электронной цифровой подписи

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. Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и её составляющие					
1.1	Понятие информационной безопасности, ее основные составляющие /Тема/	8	0			
1.2	Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем /Лек/	8	2	ПК-2.1-З ПК-2.1-У ПК-2.1-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет
1.3	Понятие информационной безопасности, ее основные составляющие /Ср/	8	3	ПК-2.1-З ПК-2.1-У ПК-2.1-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет
	Раздел 2. Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и её составляющие					
2.1	Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и её	8	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/	8	2	ПК-2.1-З ПК-2.1-У ПК-2.1-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет

2.3	Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и её составляющие /Ср/	8	4	ПК-2.1-З ПК-2.1-У ПК-2.1-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет
	Раздел 3. Законодательный уровень информационной безопасности. Административный уровень информационной безопасности. Процедурный уровень информационной безопасности					
3.1	Законодательный уровень информационной безопасности. Административный уровень информационной безопасности /Тема/	8	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/	8	2	ПК-2.2-З ПК-2.2-У ПК-2.2-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет
3.3	Законодательный уровень информационной безопасности. Административный уровень информационной безопасности /Ср/	8	4	ПК-2.2-З ПК-2.2-У ПК-2.2-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет
	Раздел 4. Процедурный уровень информационной безопасности					
4.1	Процедурный уровень информационной безопасности /Тема/	8	0			
4.2	Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ /Лек/	8	2	ПК-2.1-З ПК-2.1-У ПК-2.1-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные работы, зачет
4.3	Процедурный уровень информационной безопасности /Ср/	8	4	ПК-2.1-З ПК-2.1-У ПК-2.1-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет
	Раздел 5. Основные характеристики программно-технических мер. Идентификация и аутентификация					
5.1	Основные характеристики программно-технических мер. Идентификация и аутентификация /Тема/	8	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/	8	2	ПК-2.1-З ПК-2.1-У ПК-2.1-В	Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет
5.3	Идентификация и аутентификация /Лаб/	8	4	ПК-2.1-З ПК-2.1-У ПК-2.1-В	Л1.2 Л1.3 Л1.4Л2.1Л3.1	Отчет о выполнении лабораторной работы
5.4	Основные характеристики программно-технических мер. Идентификация и аутентификация /Ср/	8	4	ПК-2.1-З ПК-2.1-У ПК-2.1-В	Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет

	Раздел 6. Протоколирование и аудит, шифрование, контроль целостности					
6.1	Протоколирование и аудит, шифрование, контроль целостности /Тема/	8	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/	8	2	ПК-2.2-З ПК-2.2-У ПК-2.2-В	Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет
6.3	Шифрование /Лаб/	8	4	ПК-2.2-З ПК-2.2-У ПК-2.2-В	Л1.2 Л1.3 Л1.4Л2.1Л3.1	Отчет о выполнении лабораторной работы
6.4	Криптография /Лаб/	8	4	ПК-2.2-З ПК-2.2-У ПК-2.2-В	Л1.2 Л1.3 Л1.4Л2.1Л3.1	Отчет о выполнении лабораторной работы
6.5	Протоколирование и аудит, шифрование, контроль целостности /Ср/	8	4	ПК-2.2-З ПК-2.2-У ПК-2.2-В	Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет
	Раздел 7. Экранирование, анализ защищенности. Обеспечение высокой доступности					
7.1	Экранирование, анализ защищенности /Тема/	8	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/	8	2	ПК-2.2-З ПК-2.2-У ПК-2.2-В	Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет
7.3	Экранирование /Лаб/	8	4	ПК-2.2-З ПК-2.2-У ПК-2.2-В	Л1.2 Л1.3 Л1.4Л2.1Л3.1	Отчет о выполнении лабораторной 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/	8	4	ПК-2.2-З ПК-2.2-У ПК-2.2-В	Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет
	Раздел 8. Обеспечение высокой доступности					
8.1	Обеспечение высокой доступности /Тема/	8	0			
8.2	Эффективность услуг. Время недоступности. Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Обеспечение обслуживаемости. Туннелирование /Лек/	8	2	ПК-2.2-З ПК-2.2-У ПК-2.2-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет
8.3	Обеспечение высокой доступности /Ср/	8	4	ПК-2.2-З ПК-2.2-У ПК-2.2-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1	Контрольные вопросы, зачет
	Раздел 9. Промежуточная аттестация					
9.1	Подготовка к зачету, иная контактная работа /Тема/	8	0			

9.2	Прием зачета /ИКР/	8	0,25	ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-2.2-З ПК-2.2-У ПК-2.2-В	Л1.1 Л1.2 Л1.4Л2.1Л3.1	
9.3	Подготовка к зачету /Зачёт/	8	8,75	ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-2.2-З ПК-2.2-У ПК-2.2-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1	

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
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	Спицын В. Г.	Информационная безопасность вычислительной техники : учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011, 148 с.	978-5-4332-0020-3, http://www.iprbookshop.ru/13936.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

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
Операционная система Windows	Коммерческая лицензия
ABC NET	Свободное ПО
Visual studio community	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