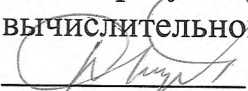


МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра «Космические технологии»

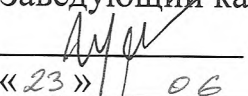
«СОГЛАСОВАНО»

Декан факультета
вычислительной техники

Д.А. Перепелкин
«25» 06 2020 г.



«УТВЕРЖДАЮ»

Проректор РОПиМД
А.В. Корячко
«25» 06 2020 г.

Заведующий кафедрой КТ

С.И. Гусев
«23» 06 2020 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

Б1.В.ДВ.02.01 «Методы и средства защиты информации»

Направление подготовки - 02.03.01 «Математика и компьютерные науки»

ОПОП академического бакалавриата
«Математика и компьютерные науки»

Квалификация (степень) выпускника — бакалавр
Форма обучения — очная

Рязань 2020

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа является составной частью основной профессиональной образовательной программы по направлению 02.03.01 «Математика и компьютерные науки», разработанной в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению 02.03.01 «Математика и компьютерные науки», утвержденным приказом Минобрнауки России № 807 от 23.08.2017.

Разработчик:

к.т.н., доцент кафедры ИБ  М.Е. Ильин

Программа рассмотрена и одобрена на заседании кафедры ИБ

« 20 » июня 2020 г., протокол № 0.

Заведующий кафедрой ИБ  В.Н. Пржегорлинский

1 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Рабочая программа по дисциплине «Методы и средства защиты информации» является составной частью основной профессиональной образовательной программы (ОПОП) бакалавриата «Математическое обеспечение и администрирование информационных систем», разработанной в соответствии с ФГОС ВО по направлению подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем.

Целью изучения дисциплины «Методы и средства защиты информации» является приобретение студентами теоретических знаний и практических навыков защиты информации представленной в электронном виде, изучение комплекса проблем информационной безопасности компьютерных систем различных типов, построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны их информационных ресурсов.

Перечень планируемых результатов обучения по дисциплине

Коды компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<p><u>Знать:</u> основные понятия и определения, используемые при изучении информационной безопасности;</p> <p><u>Уметь:</u> классифицировать автоматизированные системы согласно руководящим документам;</p> <p><u>Владеть:</u> методами и формами защиты информации.</p>
ПК-4	способностью к выбору архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования	<p><u>Знать:</u> классификацию угроз информационной безопасности;</p> <p><u>Уметь:</u> подключить организацию к Internet с соблюдением требований информационной безопасности;</p> <p><u>Владеть:</u> навыками прогнозирования эффективности функционирования систем информационной безопасности в соответствии со стратегией развития организации.</p>
ПК-5	готовностью к использованию современных системных программных средств: операционных систем, операционных и сетевых оболочек, сервисных программ	<p><u>Знать:</u> как организовать информационную безопасность на предприятии;</p> <p><u>Уметь:</u> анализировать направления развития информационно-коммуникационных технологий объектов защиты;</p> <p><u>Владеть:</u> навыками применения современных</p>

		методов обеспечения информационной безопасности.
--	--	--

2 Место дисциплины в структуре ОПОП

Дисциплина «Методы и средства защиты информации» относится к вариативной части блока Б1 (Б1.3.В.01б) профессионального цикла дисциплин основной образовательной программы подготовки бакалавров направления 02.03.02 «Математическое обеспечение и администрирование информационных систем».

Для изучения дисциплины обучаемый должен

знать:

- основы сетевых технологий;
- базовые понятия программирования на языке высокого уровня;

уметь:

- выполнять администрирование современных операционных систем;
- работать в современных офисных системах;

владеть:

- навыками обобщения информации.

Данная дисциплина базируется на следующих дисциплинах учебного плана: «Операционные системы и оболочки», «Современные технологии разработки интегрированных информационных систем».

Знания, полученные по освоению дисциплины «Методы и средства защиты информации» необходимы для подготовки выпускной работы.

Изучение данной дисциплины необходимо для разработчика и администратора современных программных систем.

3 Объем дисциплины 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 дисциплины составляет 4 зачетных единицы (ЗЕ), или 144 часа.

Вид учебной работы	Всего часов	Семестр
		8
Общая трудоёмкость час. зач.ед.	144 4	144 4
Контактная работа обучающихся с преподавателем (всего)	32	32
В том числе:		
Лекции	16	16
Лабораторные работы (ЛР)	16	16
Практические занятия (ПЗ)	-	-
Самостоятельная работа студентов (всего)	112	112
В том числе:		

Самостоятельные занятия	72	72
Экзамены и консультации	36	36
Консультации в семестре	4	4
Курсовой проект (работа)	-	-
Вид итогового контроля		экзамен

4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины, структурированное по темам

Раздел дисциплины	Содержание
1. Защита информации, ее составляющие и виды	Защита информации как деятельность. Виды защиты информации. Информационная безопасность и компьютеризация информационной среды. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг
2. Цели и направления защиты информации	Цели защиты информации. Направления защиты информации. Защита информации от утечки. Защита информации от несанкционированного воздействия. Защита информации от непреднамеренного воздействия.
3. Объекты защиты информации	Определение понятия объект защиты информации. Информация как объект защиты. Сущность и определение понятия информация как объекта защиты. Свойства информации как объективного явления. Информация как объект правовых отношений. Носитель информации как объект защиты. Определение понятия носитель информации и классификация носителей информации. Документированная информация и информационные ресурсы. Информационный процесс как объект защиты. Информационный процесс и информационная технология. Информационная система как средство реализации информационного процесса и комплексный объект защиты информации. Автоматизированная система как комплексный объект защиты информации. Определение понятия автоматизированная система. Классификация автоматизированных систем.

4. Условия, в которых осуществляется защита информации	Явления, действия, процессы, объекты и субъекты, характеризующие условия защиты информации. Вредоносные воздействия на объекты информационной инфраструктуры и угрозы безопасности информации. Нарушители безопасности информации.
5. Системы защиты информации для распространенных информационных систем	Обеспечения безопасности распространенных операционных систем и серверов различных сетевых протоколов. Архитектура системы безопасности операционных систем. Механизм контроля доступа. Система защиты информации Secret Net.

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

Очная форма обучения

Тема	Общая трудоемкость, всего часов	Контактная работа обучающихся с преподавателем				Самостоятельная работа обучающихся
		Всего	Лекции	Практические занятия,	Лабораторные работы	
1. Защита информации, ее составляющие и виды	22	2	2	-	-	20
2. Цели и направления защиты информации	24	4	4	-	-	20
3. Объекты защиты информации	24	4	4	-	-	20
4. Условия, в которых осуществляется защита информации	26	6	2	-	4	20
5. Системы защиты информации для распространенных информационных систем	48	16	4	-	12	32
Всего:	144	32	16	-	16	112

Виды практических лабораторных и самостоятельных работ

Тема	Вид работы	Наименование и содержание работы	Трудоемкость, часов
Тема 1. Защита информации, ее составляющие и виды	Самостоятельная работа	Изучение конспекта лекций.	2
		Изучение литературы по теме защита информации как деятельность.	2
		Изучение литературы по теме виды защиты информации.	2
		Изучение литературы по теме информационная безопасность и компьютеризация информационной среды.	4
		Изучение литературы по теме правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации.	4
		Изучение литературы по теме Пра-	4

Тема	Вид работы	Наименование и содержание работы	Трудоемкость, часов
		новые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг Консультации	2
Тема 2. Цели и направления защиты информации	Самостоятельная работа	Изучение конспекта лекций.	2
		Изучение литературы по теме цели защиты информации.	2
		Изучение литературы по теме направления защиты информации.	1
		Изучение литературы по теме защиты информации от утечки.	1
		Изучение литературы по теме защиты информации от несанкционированного воздействия.	1
		Изучение литературы по теме Защита информации от непреднамеренного воздействия.	1
		Подготовка к экзамену и консультации.	12
Тема 3. Объекты защиты информации	Самостоятельная работа	Изучение конспекта лекций.	2
		Изучение литературы по теме информация как объект защиты.	2
		Изучение литературы по теме информация как объект правовых отношений.	4
		Изучение литературы по теме документированная информация и информационные ресурсы.	2
		Изучение литературы по теме информационный процесс и информационная технология.	2
		Изучение литературы по теме автоматизированная система как комплексный объект защиты информации.	4
		Изучение литературы по теме классификация автоматизированных систем.	2
		Консультации.	2
Тема 4. Условия, в которых	Лабораторные работы	Настройка локальной политики безопасности Windows 7.	4

Тема	Вид работы	Наименование и содержание работы	Трудо- емкость, часов
осуществляется защита информации	Самостоятельная работа	<p>Изучение конспекта лекций. 2</p> <p>Подготовка к лабораторной работе. 2</p> <p>Изучение литературы по теме Явления, действия, процессы, объекты и субъекты, характеризующие условия защиты информации. 1</p> <p>Изучение литературы по теме. Вредоносные воздействия на объекты информационной инфраструктуры и угрозы безопасности информации. 1</p> <p>Изучение литературы по теме Нарушители безопасности информации. 2</p> <p>Подготовка к экзамену и консультации 12</p>	
5. Системы защиты информации для распространенных информационных систем	Лабораторные работы	<p>Система защиты информации Secret Net. Настройка основных функций средств разграничения доступа субъектов доступа к объектам доступа на автономной ПЭВМ. 4</p> <p>Система защиты информации Secret Net. Настройка средств контроля целостности и создания изолированной программной среды на автономной ПЭВМ. 4</p> <p>Система защиты информации Secret Net. Настройка дополнительных функций средств разграничения доступа субъектов доступа к объектам доступа. 4</p>	

Тема	Вид работы	Наименование и содержание работы	Трудо- емкость, часов
	Самостоятельная работа	Изучение конспекта лекций.	2
		Подготовка к лабораторным работам.	6
		Изучение литературы по теме обеспечения безопасности распространенных операционных систем и серверов различных сетевых протоколов.	2
		Изучение литературы по теме архитектура системы безопасности операционных систем.	2
		Изучение литературы по теме механизм контроля доступа.	2
		Изучение литературы по теме типы атак и угроз. Активные и пассивные противники.	2
		Изучение литературы по теме основные атаки и угрозы информационным системам.	2
		Изучение литературы по теме система защиты информации Secret Net.	2
		Подготовка к экзамену и консультации.	12

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

1. Бабаев С.И. Сети ЭВМ и телекоммуникаций: Учеб. пособие / РГРТУ. - Рязань 2014 - 80с.
2. Колесенков А.Н., Конкин Ю.В. Основы сетевых технологий: учеб. пособие / РГРТУ. - Рязань 2015 - 65 с.
3. Пржегорлинский В.Н., Бабаев С.И., Калинкина Т.И Компьютерные сети: метод. указ к лаб. работам / РГРТУ. - Рязань, 2015. – 80с.

6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств приведен в Приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «Методы и средства защиты информации»).

7 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная учебная литература

1. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. – Электрон. текстовые дан. – Москва: ДМК Пресс, 2014. – 702 с. – Режим доступа: <http://www.iprbookshop.ru/29257>.
2. Ветров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/

- Петров С.В., Кисляков П.А.— Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: <http://www.iprbookshop.ru/33857>.
3. Соколов, М. С. Информация как объект информационной безопасности [Электронный ресурс] / М.С. Соколов // Закон и право. – 2013. – № 12. – С. 27-33. – Режим доступа: <http://elibrary.ru/item.asp?id=20780302>
 4. Бабаев С.И. Сети ЭВМ и телекоммуникаций: Учеб. пособие / РГРТУ. - Рязань 2014 - 80с.
 5. Колесенков А.Н., Конкин Ю.В. Основы сетевых технологий: учеб. пособие / РГРТУ. - Рязань 2015 - 65 с.
 6. Пржегорлинский В.Н., Бабаев С.И., Калинкина Т.И Компьютерные сети: метод. указ к лаб. работам / РГРТУ. - Рязань, 2015. – 80с.

Дополнительная учебная литература

1. Кияев В., Граничин О. Безопасность информационных систем: курс. - Национальный Открытый Университет «ИНТУИТ», 2016 г. - 192 с.
2. Кузнецов И. Н. Бизнес-безопасность. - Издательско-торговая корпорация «Дашков и К°», 2016 г. - 416 с.
3. Балдин К. В., Уткин В. Б. Информационные системы в экономике: учебник. - Издательско-торговая корпорация «Дашков и К°», 2017 г. - 395 с.
4. Загинайлов Ю. Н. Основы информационной безопасности: учебное пособие. - Директ-Медиа, 2015 г. - 105 с.
5. Лапина М. А., Ревин А. Г., Лапин В. И. Информационное право: учебное пособие. - Юнити-Дана, 2015 г. - 336 с.
6. Хаулет Т. Инструменты безопасности с открытым исходным кодом. - Национальный Открытый Университет «ИНТУИТ», 2016 г. – 566 с.
7. Лапоница О. Р. Криптографические основы безопасности. - Национальный Открытый Университет «ИНТУИТ», 2016 г. - 244 с.

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

Обучающимся предоставлена возможность индивидуального доступа к следующим электронно-библиотечным системам:

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

9 Методические указания для обучающихся по освоению дисциплины

Рекомендации по планированию и организации времени, необходимого для изучения дисциплины

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

- Изучение конспекта лекции в тот же день, после лекции (10 – 15 минут).
- Изучение конспекта лекции за день перед следующей лекцией (10 – 15 минут).
- Изучение теоретического материала по учебнику и конспекту (1 час в неделю).

Описание последовательности действий студента («сценарий изучения дисциплины»)

При изучении дисциплины рекомендуется самостоятельно изучать материал, который еще не прочитан на лекции и не применялся на лабораторном занятии. Тогда лекция будет гораздо понятнее. Но легче при изучении курса следовать изложению материала на лекции. Для понимания материала и качественного его усвоения рекомендуется следующая последовательность действий.

1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня (10 – 15 минут).

2. При подготовке к лекции следующего дня нужно просмотреть текст предыдущей лекции, подумать о том, какой может быть тема следующей лекции (10 – 15 минут).

В течение недели выбрать время (1 час) для работы с литературой.

Рекомендации по работе с литературой

Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта изучаются и книги по теории принятия решений. Литературу по дисциплине необходимо читать только в бумажном (не в электронном) виде. Полезно использовать несколько учебников и пособий по дисциплине. Рекомендуется после изучения очередного параграфа ответить на несколько вопросов по данной теме. Кроме того, полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): «о чем этот параграф?», «какие новые понятия введены, каков их смысл?».

10 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При проведении занятий по дисциплине используются следующие информационные технологии:

– удаленные информационные коммуникации между студентами и преподавателем, ведущим лекционные и практические занятия, посредством информационной образовательной среды ФГБОУ ВО «РГРТУ», позволяющие осуществлять оперативный контроль графика выполнения и содержания образовательного процесса, решение организационных вопросов, консультирование;

– доступ к современным профессиональным базам данных (в том числе международным реферативным базам данных научных изданий) и информационным справочным системам.

Перечень лицензионного программного обеспечения:

- 1) Операционная система Windows XP Professional (лицензия Microsoft DreamSpark Membership ID 700102019);
- 2) Open Office (лицензия Apache License, Version 2.0);
- 3) Системы Secret Net демо версия.

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

- 1) Интерактивная доска.
- 2) Мультимедиа-проектор.