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

Кафедра автоматизированных систем управления

«СОГЛАСОВАНО»

Директор института
магистратуры и аспирантуры
_____ О.А. Бодров
«_25_»_____06_____2020 г.

Заведующий кафедрой АСУ
_____ Холопов С.И.
«_25_»_____06_____2020 г.

«УТВЕРЖДАЮ»

Проректор РОПиМД
_____Корячко А.В.
«_29_»_____06_____2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.09 «Программные средства защиты информации»

Направление подготовки

09.04.02 «Информационные системы и технологии»

Уровень подготовки – академическая магистратура

Квалификация выпускника – магистр

Форма обучения – очная

Рязань 2020 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.04.02 «Информационные системы и технологии», утвержденного приказом Минобрнауки России от 19.09.2017 г. № 917.

Разработчик доцент кафедры АСУ  Аникеев С.В.

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

Заведующий кафедрой
автоматизированных систем управления  Холопов С.И.

1 Цели и задачи изучения дисциплины. Перечень планируемых результатов обучения

Рабочая программа по дисциплине «Программные средства защиты информации» составлена в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования по направлению подготовки 09.04.02 «Информационные системы и технологии» (уровень магистратуры), утвержденным приказом Минобрнауки России от 19.09.2017 г. № 917.

Цель изучения дисциплины – формирование у магистрантов знаний о современных программных средствах защиты информации в компьютерных системах, овладение методами решения профессиональных задач.

Задачами дисциплины в соответствии с указанной целью являются:

- формирование у магистрантов теоретических знаний в области информационных технологий и компьютерной безопасности, а также управления информационными ресурсами; прикладных знаний в области создания и использования программных систем защиты информации; навыков самостоятельного использования соответствующих инструментальных программных систем;

- формирование у магистрантов практических навыков ограничения использования ресурсов компьютера на основе раздельного доступа пользователей, организации регистрации пользователей в сетевой операционной системе, организации защиты информации в локальной сети на уровнях входа в сеть и системы прав доступа, организации безопасной работы в Интернет и отправки почтовых сообщений в глобальной сети, использования средств защиты данных от разрушающих программных воздействий компьютерных вирусов.

2 Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Программные средства защиты информации» относится к обязательной части блока 1 (Б1.О.09) основной профессиональной образовательной программы (ОПОП). Дисциплина изучается на втором курсе в первом семестре.

Изучение данной дисциплины базируется на освоении магистрантами дисциплин «Информатика», «Технология программирования», «Проектирование информационных систем» базовой части цикла направления подготовки «Информационные системы и технологии» (бакалавриат).

Дисциплина «Программные средства защиты информации» является базой для всех последующих дисциплин профессионального цикла, научно-исследовательской практики, .а также для написания магистерской выпускной квалификационной работы.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ОПОП по направлению подготовки 09.04.02 «Информационные системы и технологии».

Общепрофессиональные компетенции выпускников и индикаторы их достижения

Код и наименование компетенции	**Код и наименование индикатора достижения общепрофессиональной компетенции**
ОПК-2- Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ИД-1$_{ОПК-2}$ Знать: современные интеллектуальные технологии получения, хранения, переработки и трансляции информации средствами современных программных средств защиты информации. ИД-2$_{ОПК-2}$ Уметь: использовать программные средства защиты информации для получения, хранения, переработки и трансляции информации, в том числе, в глобальных компьютерных сетях. ИД-3$_{ОПК-2}$ Владеть методами и средствами разработки оригинальных алгоритмов и программных средств в области построения систем защиты информации.

4 Структура и содержание дисциплины

4.1 Объем дисциплины по семестрам (курсам) и видам занятий в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Вид учебной работы	**Всего часов**
	Очная форма
Аудиторные занятия (всего)	**32,25**
В том числе: Лекции	16
Лабораторные работы (ЛР)	8
Практические занятия (ПЗ)	8
Иная контактная работа (ИКР)	0,25
Самостоятельная работа (всего)	**75,75**
В том числе: Самостоятельные занятия	67
Контроль	8,75
Вид промежуточной аттестации	Зачет
Общая трудоемкость, час.	108
Зачетные единицы трудоемкости	3
Контактная работа (по учебным занятиям)	32,25

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

Очная форма обучения

№ п/п	Тема	Общая трудоемкость, всего часов	Контактная работа обучающихся с преподавателем				Самостоятельная работа обучающихся
			Всего	Лекции	ЛР	ПЗ	
1	Введение	6	2	2			4
2	Классификация программных средств защиты информации	18	2	2			16
3	Антивирусные программы	24	8	4	4		16
4	Криптографические средства защиты информации	36	16	4	4	8	20
5	Средства идентификации и аутентификации пользователей	24	4	4			20
Всего		**108**	**32**	**16**	**8**	**8**	**76**

4.3 Содержание дисциплины

4.3.1 Лекционные занятия

№	Наименование раздела дисциплины	Содержание раздела	Трудоемкость (час)	Формируемые компетенции	Форма контроля
1	Введение	Введение	2	ОПК-2	Зачет
2	Классификация программных средств защиты информации.	Классификация программных средств защиты информации. Средства архивации данных.	2	ОПК-2	Зачет
3	Антивирусные программы.	Антивирусные программы. Классификация компьютерных вирусов. Особенности алгоритмов работы вирусов. Среда обитания вирусов. Методы обнаружения и удаления вирусов. Классификация антивирусных программ.	4	ОПК-2	Зачет
4	Криптографические средства защиты информации.	Криптографические средства защиты информации. Симметричные криптосистемы. Криптосистемы с открытым ключом. Электронная подпись. Управление ключами.	4	ОПК-2	Зачет
5	Средства идентификации и аутентификации	Средства идентификации и аутентификации пользователей. Средства управления доступом. Протоколирование и	4	ОПК-2	Зачет

	пользователей.	аудит.			

4.3.2 Лабораторные работы

Целью лабораторных работ (ЛР) является освоение и закрепление студентами теоретических положений дисциплины «Теория информационных процессов и систем».

№ п/п	Наименование лабораторных работ	Раздел дисципли-ны	Трудоем-кость (час.)	Форми-руемые компе-тенции	Формы контроля
1	Средства защиты компьютера от вирусов. Работа с антивирусными пакетами.	Раздел 3	4	ОПК-2	Отчет по лаб. работе, зачет
2	Основы описания динамических аспектов объектно-ориентированных информационных систем с использованием диаграмм последовательностей	Раздел 4	4	ОПК-2	Отчет по лаб. работе, зачет

4.3.3 Практические занятия

Целью практических занятий (ПЗ) является освоение и закрепление студентами теоретических положений дисциплины «Теория информационных процессов и систем».

№ п/п	Номер и наименование занятия	Раздел дисципли-ны	Трудоем-кость (час.)	Форми-руемые компе-тенции	Формы контроля
1	Основы проектирования PKI	Раздел 4	2	ОПК-2	Отчет о выполнении задания практ. занятия. Зачет
2	Основы проектирования PKI	Раздел 4	2	ОПК-2	Отчет о выполнении задания практ. занятия. Зачет
3	Электронная подпись	Раздел 4	2	ОПК-2	Отчет о выполнении задания практ. занятия. Зачет
4	Управление ключами	Раздел 4	2	ОПК-2	Отчет о выполнении задания практ. занятия. Зачет

4.3.4 Самостоятельная работа

Самостоятельная работа студентов по дисциплине «Программные средства защиты информации» предназначена для развития у обучающихся навыков целенаправленного самостоятельного приобретения новых знаний и умений.

Самостоятельная работа включает в себя следующие составляющие:

- изучение теоретического материала по конспектам лекций;
- самостоятельное изучение дополнительных информационных ресурсов по темам разделов дисциплины, приведенных в п. 6 «Учебно-методическое обеспечение дисциплины»;
- выполнение заданий текущего контроля успеваемости (подготовка к лабораторным работам и сдача лабораторных работ);
- выполнение заданий по практическим занятиям;
- итоговая аттестация по дисциплине (подготовка к зачету).

Подготовка к лабораторной работе предполагает изучение лекционного материала по теме лабораторной работы и разделов «Краткие теоретические сведения» в методических указаниях к лабораторным работам (теоретическая подготовка) и проведение предварительных расчетов, необходимых для успешного выполнения лабораторной работы.

Подготовка к выполнению заданий по практическим занятиям предполагает изучение соответствующих разделов лекционного материала, учебного пособия, учебника и других источников из прилагаемого списка (п.6).

№ п/п	Тематика самостоятельной работы	Трудоем-кость (час.)	Форми-руемые компе-тенции	Формы контроля
1	Подготовка по разделу 11 Введение	4	ОПК-2	ПЗ, зачет
2	Подготовка по разделу 2 Классификация программных средств защиты информации.	16	ОПК-2	ПЗ, зачет
3	Подготовка по разделу 3	16	ОПК-2	ПЗ, зачет

	Антивирусные программы.			
4	Подготовка по разделу 4 Авторские средства создания обучающих систем	20	ОПК-2	ПЗ, зачет
5	Подготовка по разделу 5 Средства идентификации и аутентификации пользователей.	20	ОПК-2	ПЗ, зачет

5 Оценочные материалы для проведения промежуточной аттестации обучающихся по дисциплине

Оценочные средства приведены в Приложении к рабочей программе дисциплины в документе «Оценочные материалы» по дисциплине «Программные средства защиты информации».

6 Учебно-методическое обеспечение дисциплины

6.1 Основная учебная литература:

1. Петраков А.В., Дорошенко П.С., Савлуков Н.В. Охрана и защита современного предприятия. М: Энергоатомиздат, 1999, 568 с.

2. Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам. – М.: Изд-во “Компания

3. Каторин Ю.Ф. и др. Большая энциклопедия промышленного шпионажа. – СПб.: ООО «Изд-во «Полигон», 2000. – 896 с.

6.2 Дополнительная учебная литература:

1. Домашев А.В., Грунтович М.М., Попов В.О. Программирование алгоритмов защиты информации. – М.: Издательство «Нолидж», 2002.

2. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002.

3. Вильям Столлингс Криптографическая защита сетей. – М.: Издательский дом «Вильямс», 2001.

6.3 Методические рекомендации по организации изучения дисциплины

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

После изучения отдельных разделов дисциплины осуществляется проведение текущего и рубежного контроля усвоения материала студентами путем тестовых вопросов.

7 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/.

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

8.1 Операционная система Windows XP (Microsoft Imagine, номер подписки ID 700565239, бессрочно).

8.2 Пакеты программного обеспечения общего назначения (текстовые редакторы, графические редакторы и др.).

8.3 Антивирусные программы Microsoft Windows Security Essentials, Avast Free Antivirus, Kaspersky Free;

8.4 OpenSSL – Cryptography and SSL/TLS toolkit (GPL) (https://www.openssl.org).

9 Материально-техническое обеспечение дисциплины

Для данной дисциплины применяется следующее материально-техническое обеспечение. *(в соответствии с МТО кафедры)*

1. Лекционные занятия:

№	Наименование специальных помещений и помещений для самостоятельной работы	Перечень специализированного оборудования
1	Учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, № 254	Персональный компьютер Celeron 2400-4 1 – шт. Проектор Toshiba TDP-T45 – 1 шт. Экран с эл. приводом Matte White S140 – 1 шт. Доска магнитно-маркерная 120*200 см Возможность подключения к сети «Интернет» проводным и беспроводным способом и обеспечением доступа в электронную информационно-образовательную среду РГРТУ.

- комплект электронных презентаций;
- аудитория, оснащенная презентационной техникой (проектор, экран, компьютер;

2. Практические занятия:

- Специализированный класс персональных ЭВМ (совместимые с IBM PC).
- презентационная техника (проектор, экран, компьютер);

3. Лабораторные работы:

- лаборатории 118, 127 оснащенные персональными компьютерами;

Прочее:

- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.