МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. УТКИНА»

Кафедра «Автоматики и информационных технологий в управлении»

«СОГЛАСОВАНО»
Заведующий кафедрой АИТУ
_____ /П.В. Бабаян/
18 ____05____ 2023 г.

«УТВЕРЖДАЮ»
Проректор по учебной работе
_____ /А.В. Корячко/
26 ____05____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки
01.03.02 Прикладная математика и информатика

Направленность (профиль) подготовки
Программирование и анализ данных

Квалификация выпускника – бакалавр

Формы обучения – очная

Рязань 2023

Общая трудоемкость **4 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
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.	50,35	50,35	50,35	50,35
Контактная работа	50,35	50,35	50,35	50,35
Сам. работа	49	49	49	49
Часы на контроль	44,65	44,65	44,65	44,65
Итого	144	144	144	144

Программу составил(и):
к.т.н., доц., Смирнов Сергей Александрович

Рабочая программа дисциплины
Основы информационной безопасности

разработана в соответствии с ФГОС ВО:
ФГОС ВО - бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика (приказ Минобрнауки России от 10.01.2018 г. № 9)

составлена на основании учебного плана:
01.03.02 Прикладная математика и информатика
утвержденного учёным советом вуза от 28.04.2023 протокол № 11.

Рабочая программа одобрена на заседании кафедры
Автоматики и информационных технологий в управлении

Протокол от 18.05.2023 г. № 7
Срок действия программы: 2023-2024 уч.г.
Зав. кафедрой Бабаян Павел Вартанович

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры
Автоматики и информационных технологий в управлении

Протокол от __ _____ 2024 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Автоматики и информационных технологий в управлении

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
Автоматики и информационных технологий в управлении

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

Автоматики и информационных технологий в управлении

Протокол от __ _____ 2027 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью освоения дисциплины «Основы информационной безопасности» является изучение основных принципов информационной безопасности, а также тенденций развития разрушающих программных воздействий.
1.2	Задачи дисциплины: изучение нормативной базы и системы международных и национальных стандартов в области информационной безопасности; ознакомление с механизмами проведения атак на программные системы, основанные на использовании стохастических методов; изучение превентивных методов защиты от разрушающих программных воздействий.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)
2.1.2	Учебная практика
2.1.3	Информатика
2.1.4	Ознакомительная практика
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Вычислительные машины и микропроцессорная техника
2.2.2	Выполнение и защита выпускной квалификационной работы
2.2.3	Преддипломная практика
2.2.4	Производственная практика

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

ОПК-4: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

ОПК-4.1. Понимает принципы работы современных информационных технологий

Знать
знать основные принципы работы современных информационных технологий

Уметь
использовать программное обеспечение при решении задач профессиональной деятельности, соблюдая требования информационной безопасности

Владеть
современными программными средствами при решении задач профессиональной деятельности, соблюдая требования информационной безопасности

ОПК-4.2. Использует современные информационные технологии для решения задач профессиональной деятельности

Знать
современные информационные технологии, используемые при решении задач профессиональной деятельности

Уметь
использовать современные информационные технологии при решении задач профессиональной деятельности, соблюдая требования информационной безопасности

Владеть
информационными технологиями при решении задач профессиональной деятельности, соблюдая требования информационной безопасности

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	тенденции развития угроз информационной безопасности, перспективные методы противодействия вредоносным программам
3.2	**Уметь:**
3.2.1	эффективно организовать свою практическую деятельность с учетом потенциальных угроз несанкционированного доступа третьих лиц, обеспечить целостность, аутентичность и избежание утечек информации при работе в Интернет и с базами данных
3.3	**Владеть:**
3.3.1	навыками и технологиями безопасного программирования, использования и настройки программного антивирусного и антипиратского программного обеспечения

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Форма контроля**
	Раздел 1. Основы информационной безовасности					
1.1	Стохастическая компьютерная вирусология /Тема/	5	0			Экзамен
1.2	Стохастическая компьютерная вирусология /Лек/	5	6	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В	Л1.3 Л1.5 Л1.6Л2.6 Л2.7 Л2.10 Э1 Э2 Э3 Э4 Э5	Экзамен
1.3	Стохастическая компьютерная вирусология /Пр/	5	2	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В	Л1.3 Л1.5 Л1.6Л2.2 Л2.9 Э1 Э2 Э3 Э4 Э5	Экзамен
1.4	Стохастическая компьютерная вирусология /Ср/	5	11	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В	Л1.3 Л1.5 Л1.6Л2.7 Л2.10 Э1 Э2 Э3 Э4 Э5	Экзамен
1.5	Тенденции развития угроз информационной безопасности /Тема/	5	0			Экзамен
1.6	Тенденции развития угроз информационной безопасности /Лек/	5	10	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В	Л1.3 Л1.7Л2.10 Э2 Э3 Э4 Э5	Экзамен
1.7	Тенденции развития угроз информационной безопасности /Пр/	5	4	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В	Л1.3Л2.5 Л2.8 Л2.10 Э2 Э3 Э4 Э5	Экзамен
1.8	Тенденции развития угроз информационной безопасности /Ср/	5	12	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В	Л1.3 Л1.7Л2.5 Л2.8 Л2.10 Э2 Э3 Э4 Э5	Экзамен
1.9	Скрытые каналы передачи данных /Тема/	5	0			Экзамен
1.10	Скрытые каналы передачи данных /Лек/	5	12	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В	Л1.1 Л1.2 Л1.4 Л1.8Л2.1 Л2.3 Л2.4 Э2 Э3 Э4 Э5	Экзамен
1.11	Скрытые каналы передачи данных /Пр/	5	4	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В	Л1.1 Л1.2 Л1.4 Л1.8Л2.1 Л2.8 Э2 Э3 Э4 Э5	Экзамен

1.12	Скрытые каналы передачи данных /Ср/	5	18	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В	Л1.1 Л1.2 Л1.4 Л1.8Л2.1 Л2.3 Л2.4 Э2 Э3 Э4 Э5	Экзамен
1.13	Технология безопасного программирования /Тема/	5	0			Экзамен
1.14	Технология безопасного программирования /Лек/	5	4	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В	Л1.1 Л1.2 Л1.4 Л1.8Л2.1 Э2 Э3 Э4 Э5	Экзамен
1.15	Технология безопасного программирования /Пр/	5	6	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В	Л1.1 Л1.2 Л1.4 Л1.8Л2.3 Л2.4 Э2 Э3 Э4 Э5	Экзамен
1.16	Технология безопасного программирования /Ср/	5	8	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В	Л1.1 Л1.2 Л1.4 Л1.8Л2.1 Л2.3 Л2.4 Э2 Э3 Э4 Э5	Экзамен
	Раздел 2. Промежуточная аттестация					
2.1	Подготовка и сдача зачета /Тема/	5	0			
2.2	Консультация перед экзаменом /Кнс/	5	2	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В		
2.3	Сдача экзамена /ИКР/	5	0,35	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В		
2.4	Подготовка к экзамену /Экзамен/	5	44,65	ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы приведены в приложении к рабочей программе дисциплины (см. документ "Оценочные материалы по дисциплине "Основы информационной безопасности")

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	Новиков С. Н., Солонская О. И.	Методы защиты информации : учебное пособие	Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2009, 121 с.	2227-8397, http://www.iprbookshop.ru/54767.html
Л1.2	Астайкин А. И., Мартынов А. П., Николаев Д. Б., Фомченко В. Н.	Методы и средства обеспечения программно-аппаратной защиты информации : научно-техническое издание	Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015, 224 с.	978-5-9515-0305-3, http://www.iprbookshop.ru/60959.html
Л1.3	Бехроуз А., Берлин А. Н.	Криптография и безопасность сетей : учебное пособие	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017, 782 с.	978-5-4487-0143-6, http://www.iprbookshop.ru/72337.html
Л1.4	Джонс К. Д., Шема М., Джонсон Б. С.	Инструментальные средства обеспечения безопасности	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, 914 с.	2227-8397, http://www.iprbookshop.ru/73679.html
Л1.5	Суворова Г. М.	Информационная безопасность : учебное пособие	Саратов: Вузовское образование, 2019, 214 с.	978-5-4487-0585-4, http://www.iprbookshop.ru/86938.html
Л1.6	Петров А. А.	Компьютерная безопасность. Криптографические методы защиты	Саратов: Профобразование, 2019, 446 с.	978-5-4488-0091-7, http://www.iprbookshop.ru/87998.html
Л1.7	Сергиенко Е. Н.	Математические методы кодирования и шифрования : учебное пособие	Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2017, 101 с.	2227-8397, http://www.iprbookshop.ru/92262.html
Л1.8	Червяков Н. И., Бабенко М. Г., Гладков А. В.	Вероятностные методы оценки состояния информационной безопасности : учебное пособие	Ставрополь: Северо-Кавказский федеральный университет, 2017, 182 с.	2227-8397, http://www.iprbookshop.ru/92536.html
6.1.2. Дополнительная литература				

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Симонян А. Г.	Учебно-методическое пособие по дисциплине Методы и средства защиты компьютерной информации	Москва: Московский технический университет связи и информатики, 2016, 32 с.	2227-8397, http://www.iprbookshop.ru/61498.html
Л2.2	Котов Ю. А.	Криптографические методы защиты информации. Шифры : учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2016, 59 с.	978-5-7782-2959-4, http://www.iprbookshop.ru/91377.html
Л2.3	Смирнов А. Э., Пономарёва Ю. А.	Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации	Москва: Московский технический университет связи и информатики, 2015, 67 с.	2227-8397, http://www.iprbookshop.ru/61738.html
Л2.4	Симонян А. Г., Режеб Т. Б. К.	Практикум по выполнению лабораторных работ по дисциплине Методы и средства защиты компьютерной информации	Москва: Московский технический университет связи и информатики, 2015, 58 с.	2227-8397, http://www.iprbookshop.ru/61743.html
Л2.5	Пашинцев В. П., Ляхов А. В.	Нестандартные методы защиты информации : лабораторный практикум	Ставрополь: Северо-Кавказский федеральный университет, 2016, 196 с.	2227-8397, http://www.iprbookshop.ru/63217.html
Л2.6	Котова Л. В.	Сборник задач по дисциплине «Методы и средства защиты информации» : учебное пособие	Москва: Московский педагогический государственный университет, 2015, 44 с.	978-5-4263-0221-1, http://www.iprbookshop.ru/70020.html
Л2.7	Тебуева Ф. Б., Антонов В. О.	Теоретико-числовые методы в криптографии : учебное пособие	Ставрополь: Северо-Кавказский федеральный университет, 2017, 107 с.	2227-8397, http://www.iprbookshop.ru/75601.html
Л2.8	Кирпичников А. П., Хайбуллина З. М.	Криптографические методы защиты компьютерной информации : учебное пособие	Казань: Казанский национальный исследовательский технологический университет, 2016, 100 с.	978-5-7882-2052-9, http://www.iprbookshop.ru/79313.html
Л2.9	Бондаренко И. С., Демчишин Ю. В.	Методы и средства защиты информации : лабораторный практикум	Москва: Издательский Дом МИСиС, 2018, 32 с.	2227-8397, http://www.iprbookshop.ru/84413.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.10	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019, 702 с.	978-5-4488-0070-2, http://www.iprbookshop.ru/87995.html

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Официальный интернет портал РГРТУ [электронный ресурс] http://www.rsreu.ru
Э2	Образовательный портал РГРТУ [электронный ресурс]. - Режим доступа: по паролю.- https://edu.rsreu.ru
Э3	Электронная библиотека РГРТУ [электронный ресурс]. - Режим доступа: доступ из корпоративной сети РГРТУ - по паролю. - http://elib.rsreu.ru/
Э4	Электронно-библиотечная система IRPbooks [электронный ресурс]. - Режим доступа: доступ из корпоративной сети РГРТУ - свободный, доступ из сети интернет- по паролю. - https://www.iprbookshop.ru/
Э5	Электронно-библиотечная система «Лань» [электронный ресурс]. - Режим доступа: доступ из корпоративной сети РГРТУ - свободный, доступ из сети интернет- по паролю. - https://e.lanbook.com

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
Kaspersky Endpoint Security	Коммерческая лицензия
Adobe Acrobat Reader	Свободное ПО
LibreOffice	Свободное ПО
Firefox	Свободное ПО
7 Zip	Свободное ПО

6.3.2 Перечень информационных справочных систем

6.3.2.1	Информационно-правовой портал ГАРАНТ.РУ http://www.garant.ru
6.3.2.2	Система КонсультантПлюс http://www.consultant.ru
6.3.2.3	Справочная правовая система «КонсультантПлюс» (договор об информационной поддержке №1342/455-100 от 28.10.2011 г.)

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1	445 учебно-административный корпус. Учебная аудитория для проведения учебных занятий лекционного и семинарского типа, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Специальная мебель (54 посадочных места), компьютер с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду РГРТУ, мультимедиа проектор, экран, доска, колонки звуковые.
2	449 учебно-административный корпус. Учебная аудитория для проведения учебных занятий семинарского типа, лабораторных работ, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 15 компьютеров с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду РГРТУ, проектор, экран, доска, магнитный усилитель, фазовращатель, асинхронные приводы, осциллограф, электронный микроскоп, учебный роботизированный стенд, учебный комплект роботизированного оборудования Mindstorms, видеокамера
3	447 учебно-административный корпус. Помещение для самостоятельной работы обучающихся 10 компьютеров с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду РГРТУ, учебный роботизированный стенд, видеокамеры, сервер данных

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Методическое обеспечение дисциплины приведено в приложении к рабочей программе дисциплины (см. документ "Методические указания дисциплины "Основы информационной безопасности")

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Ф. УТКИНА

Кафедра «Автоматики и информационных технологий в управлении»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление 01.03.02
«Прикладная математика и информатика»

ОПОП
«Программирование и анализ данных»

Квалификация выпускника – бакалавр

Формы обучения – очная

Рязань 2023

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

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций обучающихся целям и требованиям основной профессиональной образовательной программы в ходе проведения текущего контроля и промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных, общепрофессиональных и профессиональных компетенций, приобретаемых обучающимся в соответствии с этими требованиями.

Контроль знаний проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости проводится с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся и принятия необходимых мер по совершенствованию методики преподавания учебной дисциплины, организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков, приобретенных обучающимися в ходе выполнения индивидуальных заданий на практических занятиях. При оценивании результатов освоения практических занятий применяется шкала оценки «зачтено – не зачтено». Количество практических работ и их тематика определена рабочей программой дисциплины, утвержденной заведующим кафедрой.

Результат выполнения каждого индивидуального задания должен соответствовать всем критериям оценки в соответствии с компетенциями, установленными для заданного раздела дисциплины.

Промежуточный контроль по дисциплине осуществляется проведением экзамена.

Форма проведения экзамена – письменный ответ по утвержденным экзаменационным билетам, сформулированным с учетом содержания учебной дисциплины. После выполнения письменной работы обучаемого производится ее оценка преподавателем и, при необходимости, проводится теоретическая беседа с обучаемым для уточнения экзаменационной оценки.

Паспорт оценочных материалов по дисциплине

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по темам)	Код контролируемой компетенции (или её части)	Вид, метод, форма оценочного мероприятия
1	2	3	4
1	**Тема 1. Стохастическая компьютерная вирусология**	ОПК-4.1– З ОПК-4.1– У ОПК-4.1– В ОПК-4.2– З ОПК-4.2– У ОПК-4.2– В	Экзамен
2	**Тема 2. Тенденции развития угроз информационной безопасности**	ОПК-4.1– З ОПК-4.1– У ОПК-4.1– В ОПК-4.2– З ОПК-4.2– У ОПК-4.2– В	Экзамен
3	**Тема 3. Скрытые каналы передачи данных**	ОПК-4.1– З ОПК-4.1– У ОПК-4.1– В ОПК-4.2– З ОПК-4.2– У ОПК-4.2– В	Экзамен
4	**Тема 4. Технология безопасного программирования**	ОПК-4.1– З ОПК-4.1– У ОПК-4.1– В ОПК-4.2– З ОПК-4.2– У ОПК-4.2– В	Экзамен

Критерии оценивания компетенций (результатов)

1). Уровень усвоения материала, предусмотренного программой.

2). Умение анализировать материал, устанавливать причинно-следственные связи.

3). Ответы на вопросы: полнота, аргументированность, убежденность, умение

4). Качество ответа (его общая композиция, логичность, убежденность, общая эрудиция)

5). Использование дополнительной литературы при подготовке ответов.

Уровень освоения сформированности знаний, умений и навыков по дисциплине оценивается в форме бальной отметки:

«Отлично» заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший

основную и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка «отлично» выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала.

«Хорошо» заслуживает студент, обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка «хорошо» выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.

«Удовлетворительно» заслуживает студент, обнаруживший знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справляющийся с выполнением заданий, предусмотренных программой, знакомый с основной литературой, рекомендованной программой. Как правило, оценка «удовлетворительно» выставляется студентам, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя.

«Неудовлетворительно» выставляется студенту, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Типовые контрольные задания или иные материалы

Вопросы к экзамену по дисциплине

1. Чем полиморфные вирусы отличаются от самошифрующихся?
2. Сформулируйте принцип обнаружения компьютерного вируса методом сигнатурного анализа.
3. Сформулируйте принцип обнаружения компьютерного вируса методом эвристического анализа.
4. Какой метод используется для обнаружения компьютерного вируса в момент их активизации?
5. Какой метод используется для обнаружения последствий вирусной активности?
6. Какие методы используются для обнаружения компьютерного вируса до момента их активизации?
7. Какие существуют типы программных средств антивирусной защиты?
8. Что такое вирусная сигнатура? Приведите пример.

9. Что такое эвристический признак компьютерного вируса? Приведите пример.
10. Что такое ошибка 1-го рода при работе программных средств антивирусной защиты?
11. Что такое ошибка 2-го рода при работе программных средств антивирусной защиты?
12. Что такое ошибка 3-го рода при работе программных средств антивирусной защиты?
13. Что такое клептографическая атака на криптоалгоритм?
14. Какие криптоалгоритмы могут являться объектом клептографической атаки?
15. Приведите пример клептографической атаки на криптоалгоритм RSA.
16. Как можно защититься от клептографической атаки?
17. Опишите клептографическую атаку на криптосистему Эль-Гамаля.
18. Опишите возможную клептографическую атаку на генератор ПСЧ.
19. Как вы понимаете термин «клептография»? Приведите примеры, иллюстрирующие данное понятие.
20. Что такое недоказуемое шифрование?
21. Что такое криптовычисления?
22. Каким образом можно получить запись из базы данных таким образом, чтобы не раскрывать, какая именно запись была получена?
23. Что такое отрицаемое шифрование?
24. Какие программы называют симбиотическими?
25. Приведите примеры симбиотических разрушающих программных воздействий.
26. Каким образом можно использовать сетевые разрушающие программные воздействия для проведения распределенных вычислений?
27. Предположим, что улучшенный криптотроян применяет плохой генератор случайных чисел и сеансовые ключи, сформированные на разных компьютерах, оказываются одинаковыми. Какие последствия это может иметь?
28. Какие методы противодействия автоматической рассылке сообщений вы знаете?
29. В чем различие между принципами недоказуемого и отрицаемого шифрования?
30. Какому риску подвергаются вредоносные программы, участвующие в протоколе информационного шантажа, при использовании ими некачественных генераторов случайных чисел?
31. Какую роль в протоколе контроля работоспособности узлов распределенных вычислений играет случайный бит b?
32. С какой вероятностью для достижения своих целей в протоколе безопасного выкупа жертве придется купить не более k сообщений ($1 \le k \le 2S$)?
33. Дайте определение скрытого канала передачи данных.
34. Дайте определение потайного канала передачи данных.
35. Дайте определение побочного канала передачи данных.
36. Перечислите типы скрытых каналов передачи данных.
37. Что такое скрытый канал по памяти?

38. Что такое скрытый канал по времени?
39. Какие основные характеристики скрытых каналов используются при их описании?
40. Укажите различия между синхронными и асинхронными скрытыми каналами.
41. Какое влияние оказывает синхронизация на емкость канала?
42. Укажите особенности применения скрытых каналов в системах обработки информации.
43. Перечислите методы организации локальных скрытых каналов.
44. Перечислите методы организации сетевых скрытых каналов.
45. Каким образом можно организовать скрытые каналы на базе стека протоколов TCP/IP: IP и ICMP?
46. Каким образом можно организовать скрытые каналы на базе стека протоколов TCP/IP: TCP и UDP?
47. Каким образом можно использовать протоколы уровня приложений HTTP и DNS для организации скрытых каналов?
48. Укажите методы противодействия угрозе организации скрытых каналов?
49. В чем состоят главные отличия компилятора от транслятора?
50. Перечислите преимущества трансляторов?
51. Какие интерпретируемые языки вы знаете?
52. Укажите основные особенности скрипт-вирусов.
53. Укажите методы обнаружения скрипт-вирусов.
54. Какие возможности предоставляет утилита awk?
55. Почему присутствие команды «rm» является одним из наиболее характерных признаков скрипт-вируса?
56. Какими свойствами должен обладать скрипт-файл, чтобы быть классифицированным как вирус?
57. Что такое уязвимость программного кода?
58. К каким последствиям может привести существование уязвимости в программном коде?
59. Каковы основные причины появления уязвимости в программном коде?
60. В чем суть уязвимости, вызванной переполнением буфера на стеке?
61. Укажите основные способы борьбы с уязвимостями переполнения буфера на стеке.
62. К каким последствиям может привести существование уязвимости класса «переполнение кучи»?
63. Укажите основные методы борьбы с уязвимостями класса «переполнение кучи».
64. К каким последствиям может привести существование уязвимостей класса «целочисленное переполнение»?
65. Каковы последствия существования уязвимостей в программах, написанных с использованием интерпретируемых языков?
66. В чем суть уязвимости внедрения команд?
67. К каким последствиям может привести существование уязвимости внедрения SQL-кода?

Практикум по дисциплине

№ п/п	№ темы дисциплины	Наименование практического занятия	Трудоемкость, час
1	1	Анализ механизмов функционирования компьютерных вирусов, использующих стохастические методы для сокрытия и выполнения деструктивных функций.	2
2	2	Клептографическая атака на алгоритм выработки общего секретного ключа. Защита от клептографических атак.	4
3	3	Классификация скрипт-вирусов. Поиск скрипт-вирусов на основе анализа кода. Выделение эвристических признаков скрипт-вирусов	4
4	4	Уязвимость переполнения буфера. Уязвимость строки формата. Уязвимость целочисленного переполнения. Уязвимость индексации массива. Уязвимость подключения внешних файлов. Уязвимость использования глобальных переменных. Уязвимость внедрения команд. Уязвимость внедрения SQL кода.	6

Типовые задания для самостоятельной работы

1. Анализ механизмов функционирования компьютерных вирусов, использующих стохастические методы для затруднения своего обнаружения.
2. Анализ механизмов функционирования компьютерных вирусов, использующих стохастические методы для выполнения деструктивных функций.
3. Элементы теории игр. Информационный шантаж. Распределенные вычисления. Безопасный выкуп.
4. Угроза проведения атак на Unix-системы с использованием скрипт-вирусов для командных интерпретаторов.
5. Интерпретатор и компилятор. Преимущества вирусов на интерпретируемых языках.
6. Скрипт-вирусы на языке Shell. Классификация технических приемов, используемых скрипт-вирусами.
7. Перспективные методы противодействия вредоносным программам.
8. Иммунологический подход к антивирусной защите. Понятие иммунной системы.
9. Архитектура компьютерной иммунной системы.
10. Автономность надежной системы защиты.
11. Стохастический подход к защите информации.
12. Поведенческий анализ программ. Поведение по определению. Определение по поведению.
13. Иммунологический подход. Распределенное обнаружение изменений.
14. Современные тенденции в динамическом анализе кода.