Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Первый проректор –
проректор по учебной работе
_____Н.Г. Кузнецов
«01» июня 2018 г.

Рабочая программа дисциплины

Компьютерная вирусология

по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Квалификация

Бакалавр

Ростов-на-Дону
2018 г.

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
Недель	18			
Вид занятий	УП	РПД	УП	РПД
Лекции	36	36	36	36
Лабораторные	36	36	36	36
В том числе инт.	16	16	16	16
Итого ауд.	72	72	72	72
Контактная	72	72	72	72
Сам. работа	36	36	36	36
Часы на контроль	36	36	36	36
Итого	144	144	144	144

ОСНОВАНИЕ

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 "Информационная безопасность" (уровень бакалавриата) (приказ Минобрнауки России от 01.12.2016г. №1515)

Рабочая программа составлена

по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Учебный план утвержден учёным советом вуза от 27.03.2018 протокол № 10.

Программу составил(и): *к.ф.-м.н., доцент, Шейдаков Н.Е.* _____ 11.05.18

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____ 11.05.18

Методическим советом направления *к.ф.-м.н., декан, Карасёв Д.Н.* _____ 16.05.18

Отделом образовательных программ и планирования учебного процесса Торопова Т.В. _____ 30.05.18

Проректором по учебно-методической работе Джуха В.М. _____ 31.05.18

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования
учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2019-2020 учебном году на заседании
кафедры **Информационные технологии и защита информации**

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и)*ж.ф.-м.н., доцент, Шейдаков Н.Е.* _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования
учебного процесса Торопова Т.В.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2020-2021 учебном году на заседании
кафедры **Информационные технологии и защита информации**

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): *к.ф.-м.н., доцент, Шейдаков Н.Е.* _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования
учебного процесса Торопова Т.В.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2021-2022 учебном году на заседании
кафедры **Информационные технологии и защита информации**

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): *к.ф.-м.н., доцент, Шейдаков Н.Е.* _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования
учебного процесса Торопова Т.В.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2022-2023 учебном году на заседании
кафедры **Информационные технологии и защита информации**

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): *к.ф.-м.н., доцент, Шейдаков Н.Е.* _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цели освоения дисциплины: ознакомление обучаемых с основными понятиями компьютерной вирусологии, и подготовка их к организации защиты компьютерных систем и сетей от компьютерных вирусов;
1.2	Задачи изучения дисциплины: определение роли защиты от компьютерных вирусов в системе информационной безопасности предприятия; изучение возможностей существующих программ деструктивного воздействия; оценка эффективности существующих средств защиты; изучение механизма организации централизованной антивирусной защиты; выработка навыков в области управления антивирусной защитой.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ООП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Необходимыми условиями для успешного осовения дисциплины являются навыки, знания и умения, полученные в результате изучения дисциплин:
2.1.2	Методы атакующего воздействия на информационные ресурсы
2.1.3	Методы и средства обеспечения информационной безопасности
2.1.4	Низкоуровневое программирование
2.1.5	Основы информационной безопасности
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Защита от удаленных сетевых атак
2.2.2	Комплексное обеспечение защиты информации объекта информатизации
2.2.3	Методы и средства обеспечения информационной безопасности
2.2.4	Программно-аппаратные средства защиты информации

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
Знать:
сущность предмета компьютерной вирусологии; методы
Уметь:
обнаруживать и удалять компьютерные вирусы и другие вредоносные программы
Владеть:
методами и средствами защиты от компьютерных вирусов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Интеракт.	Примечание
	Раздел 1. Основные понятия о компьютерных вирусах						
1.1	Тема 1.1. «Введение в компьютерную вирусологию»: объект, предмет и цель курса. Роль курса «Компьютерная вирусология» в системе дисциплин по защите информации. Появление термина «Компьютерный вирус», военные разра -ботки, возникновение эпидемий компьютерных вирусов. /Лек/	6	4	ПК-1	Л1.1 Л1.3 Э1 Э6 Э7 Э8	0	
1.2	Тема 1.2. « Философские и математические аспекты» Введение. Результат Фреда Коэна. Результат Д. Чесса и С. Вайта. Формализм Ф. Лейтольда. Результат Леонарда Адельмана /Лек/	6	4	ПК-1	Л1.1 Л1.2 Л1.3 Э1 Э6 Э7 Э8	0	

1.3	Тема 1.3. «Основные определения. Классификация» Определение компьютерного вируса. Отличительные особенности компьютерных вирусов и других вредоносных программ. Классификация по способу использования ресурсов. Класси-фикация по типу заражаемых объектов. Классификация по принципам активации. Классификация по способу организа-ции программного кода. Классификация по вредоносным функциям. Классификация по степени опасности. /Лек/	6	4	ПК-1	Л1.1 Л1.3 Л2.1 Э1 Э6 Э7 Э8	2	
1.4	Тема 1.4. «Файловые вирусы в Windows» Факторы опаснос ти компьютерных вирусов» Признаки наличия компьютерного вируса. /Лек/	6	4	ПК-1	Л1.1 Л1.2 Л1.3 Э1 Э7	2	
1.5	Тема 1.3. «Основные определения. Классификация» Основные признаки присутствия вредоносных программ и методы по устранению последствий вирусных заражений /Лаб/	6	4	ПК-1	Л1.1 Э1 Э2 Э6	2	
1.6	Тема 1.4. «Файловые вирусы в Windows» Разработка нерезидентной вирусной EXE-программы /Лаб/	6	4	ПК-1	Л1.1 Э1	0	
1.7	Тема 1.4. «Файловые вирусы в Windows» Разработка резидентной вирусной EXE-программы /Лаб/	6	4	ПК-1	Л1.1	0	
1.8	Тема 1.3. «Основные определения. Классификация» Файловые вирусы в MS-DOS /Ср/	6	4	ПК-1	Л1.1 Л1.2 Э1 Э2 Э3 Э6	0	
1.9	Тема 1.3. «Основные определения. Классификация» Загрузочные вирусы /Ср/	6	4	ПК-1	Л1.1 Л1.2 Э1 Э2 Э6	0	
1.10	Тема 1.4. «Файловые вирусы в Windows» Технологии заражения /Ср/	6	4	ПК-1	Л1.1 Л1.2 Э7	0	
	Раздел 2. Методы защиты от программ деструктивного воздействия						
2.1	Тема 2.1. «Что такое антивирусы» Технологии обнаружения вирусов. Режимы работы антивирусов. Антивирусный комплекс. Комплексная система защиты информации /Лек/	6	4	ПК-1	Л1.1 Л2.2 Л2.3 Э7 Э8	0	
2.2	Тема 2.2. «Защита шлюзов»: Общие сведения. Возможные схемы защиты. Требования к антивирусам для шлюзов. Угро-зы и методы защиты от них. Эксплуатационные характери- стики. /Лек/	6	4	ПК-1	Л1.1 Л1.3 Л2.3 Э2 Э8	2	
2.3	Тема 2.3. «Защита почтовых систем» Общие сведения. Возможные схемы защиты. Требования к антивирусному комплексу для проверки почтового потока. Microsoft Exchange. Unix-системы. /Лек/	6	4	ПК-1	Л1.1 Л1.3 Э6 Э7 Э8	0	

2.4	Тема 2.4. «Защита серверов и рабочих станций» Общие сведения. Защита рабочих станций. Защита серверов. Система администрирования. /Лек/	6	4	ПК-1	Л1.1 Л1.2 Л1.3 Э6 Э8	2	
2.5	Тема 2.5 «Экономические и правовые аспекты компьютерной вирусологии» Вред, наносимый компьютерными вирусами и другими вредоносными программами с точки зрения экономики» Экономические цели вирусопи-сателей. Статистические данные. Ущерб, наносимый предприятиям (орга-низациям) вирусными эпидемиями. Правовое регулирование создания и распространения компьютерных вирусов и других вредоносных про- грамм /Лек/	6	4	ПК-1	Л1.1 Л1.3 Л2.4 Э2 Э4 Э6 Э7	0	
2.6	Тема 2.3. «Защита почтовых систем» Антивирус Касперского 5.5 для MS Exchange Server. Установка, настройка, управление /Лаб/	6	4	ПК-1	Л1.1 Э1 Э2 Э7 Э8	2	
2.7	Тема 2.4. «Защита серверов и рабочих станций» Kaspersky Administration Kit. Особенности работы с иерархической структурой Серверов администрирования /Лаб/	6	4	ПК-1	Л1.1 Э1 Э2 Э7 Э8	0	
2.8	Тема 2.4. «Защита серверов и рабочих станций» Антивирус Касперского 6.0 для Windows Workstations. Локальная установка и управление /Лаб/	6	4	ПК-1	Л1.1 Э1 Э2 Э7 Э8	0	
2.9	Тема 2.4. «Защита серверов и рабочих станций» Подготовка лабораторного стенда - корпоративной сети под управлением ОС Microsoft Windows Server 2016	6	4	ПК-1	Л1.1 Э1 Э2 Э7 Э8	2	
2.10	Тема 2.4. «Защита серверов и рабочих станций» Развертывание антивирусной защиты в сети лабораторного стенда и управление задачами обеспечения антивирусной защиты на базе комплекса управления защитой Kaspersky Security Center 10 и антивируса Kaspersky Endpoint Security 10 /Лаб/	6	4	ПК-1	Л1.1 Э2 Э7 Э8	0	
2.11	Тема 2.4. «Защита серверов и рабочих станций» Подбор и развертывание сертифицированного решения для удаленного управления антивирусной защитой в корпоративной информационной сети из линейки продуктов Dr.Web Enterprise Security	6	4	ПК-1	Л1.1 Э2 Э6 Э7	2	
2.12	Тема 2.1. «Что такое антивирусы» Мобильные антивирусы: защита планшетов и телефонов /Ср/	6	4	ПК-1	Л1.1 Э3 Э4 Э5	0	
2.13	Тема 2.1. «Что такое антивирусы» Антивирусный комплекс ESET Nod32 /Ср/	6	4	ПК-1	Л1.1 Э6 Э7	0	
2.14	Тема 2.1. «Что такое антивирусы» Антивирусный комплекс DoctorWeb /Ср/	6	4	ПК-1	Л1.1 Э6 Э7	0	

2.15	Тема 2.5 «Экономические и правовые аспекты компьютерной вирусологии» Темы и вопросы, определяемые преподавателем с учетом интересов студента (рефераты) 1.Макровирусы 2.Почтовые черви 3.Вирусы, поражающие com-файлы 4.Вирусы, поражающие exe-файлы 5.Загрузочные вирусы 6.Полиморфные и Stealth-вирусы 7.Вирусы, работающие в среде Windows 8.Методы защиты от компьютерных вирусов 9.Антивирусное программное обеспечение 10.Антивирусная защита мобильных пользователей 11.Логические бомбы 12.Программы Дозвона /Ср/	6	12	ПК-1	Л1.1 Э1 Э2 Э3 Э4 Э5	0	
2.16	/Экзамен/	6	36	ПК-1	Л1.1 Л1.2 Л2.2 Э1 Э2 Э5	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

Вопросы к экзамену
1. Компьютерные вирусы. Основные определения.
2. Классификация компьютерных вирусов.
3. Обзор способов заражения компьютерных систем и сетей.
4. Макровирусы.
5. Основные принципы полиморфизма на примере макровирусов.
6. Почтовые черви.
7. Троянские программы. Общие принципы работы. Типы троянских программ.
8. Троянские программы типа Backdoor, алгоритм, структура.
9. Вирусы, поражающие com-файлы.
10. Вирусы, поражающие exe-файлы MS DOS.
11. Загрузочные (boot) вирусы.
12. Резидентные вирусы в системе MS DOS.
13. Полиморфные вирусы.
14. Stealth-вирусы.
15. Вирусы, работающие в системе Windows XP/7/2003/2008, принципы работы.
16. Методы борьбы с вирусами.
17. Антивирусные программы. Типы, примеры.
18. Антивирусные комплексы. AVP. DrWeb. EsetNod32
19. Выбор антивирусного программного средства.
20. Принципы организации антивирусной защиты предприятия.
21. Правовые аспекты компьютерной вирусологии
22. Каковы признаки заражения системы?
23. Существует ли строгая последовательность действий при заражении?
24. Нужно ли как то ограничивать доступ к носителям с этой информацией?
25. Перечислите основные методы профилактики заражения?
26. Приведите примеры наиболее известных антивирусов?
27. Как называется статья №272 УК РФ?
28. Как называется статья №273 УК РФ?
29. Как называется статья №274 УК РФ?
30. Что означает термин "компьютерная информация"?
31. Как наказывается неправомерный доступ к компьютерной информации?
32. Как наказывается то же самое, но по предварительному сговору?

5.2. Фонд оценочных средств для проведения текущего контроля

Структура и содержание фонда оценочных средств представлены в Приложении 1 к рабочей программе дисциплины

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

6.1. Рекомендуемая литература

6.1.1. Основная литература				
	Авторы,	Заглавие	Издательство,	Колич-во
Л1.1	Скудис Э.	Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите: [пер. с англ.]	М.: ДМК Пресс, 2003	102
Л1.2	Левин М.	Руководство для хакеров 2 : Электронные корсары	М.: Новый издат. дом, 2005	11
Л1.3	Михайлов А. В.	Компьютерные вирусы и борьба с ними / http://biblioclub.ru/index.php?page=book&id=136089	Москва: Диалог-МИФИ, 2012	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
6.1.2. Дополнительная литература				
	Авторы,	Заглавие	Издательство,	Колич-во
Л2.1	Яшутина О. А.	Обеспечение информационной безопасности с помощью антивируса Касперского. Лекция 1. Классификация вредоносных программ. Методы защиты. Презентация / https://biblioclub.ru/index.php?page=book_red&id=239488	Москва: Национальный Открытый Университет «ИНТУИТ»,	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л2.2	Яшутина О. А.	Обеспечение информационной безопасности с помощью антивируса Касперского. Лекция 2. Локальное использование Антивируса Касперского 6.0. Презентация / https://biblioclub.ru/index.php?page=book_red&id=239491	Москва: Национальный Открытый Университет «ИНТУИТ»,	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л2.3	Яшутина О. А.	Обеспечение информационной безопасности с помощью антивируса Касперского. Лекция 4. Антивирус Касперского для Linux File Server. Презентация / https://biblioclub.ru/index.php?page=book_red&id=239492	Москва: Национальный Открытый Университет «ИНТУИТ»,	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л2.4	Чепурнова Н. М., Ефимова Л. Л.	Правовые основы информатики: учебное пособие / https://biblioclub.ru/index.php?page=book_red&id=426501	Москва: Юнити-Дана, 2015	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"	
Э1	Вирусы и средства борьбы с ними. Курс Интернет-университета информаци-онных технологий / https://biblioclub.ru/index.php?page=book_red&id=234893
Э2	Обеспечение информационной безопасности с помощью антивируса Касперского: Видеокурс Интернет-университета информационных технологий / https://biblioclub.ru/index.php?page=book_red&id=239491
Э3	Мобильные телекоммуникации. 2015. № 4/5(138) Москва: Профи-Пресс, 2015 / https://biblioclub.ru/index.php?page=book_red&id=336189
Э4	Национальный Банковский Журнал. 2016. № 11(152) / https://biblioclub.ru/index.php?page=book_red&id=447924
Э5	Мобильные телекоммуникации. 2013. № 6 / https://biblioclub.ru/index.php?page=book_red&id=231372
Э6	Антивирусная защита компьютерных систем [Электронный ресурс] / М.:Интернет-Университет Ин-формационных Технологий,2007. -282с. / http://biblioclub.ru/index.php?page=book&id=233568
Э7	Вирусы и средства борьбы с ними: курс [Электронный ресурс] / М.:Интернет-Университет Информа-ционных Технологий,2007. -305с. / http://biblioclub.ru/index.php?page=book&id=234893
Э8	Безопасность информационных систем: курс / Кияев В. , Граничин О. Национальный Открытый Университет «ИНТУИТ», 2016, 192 стр. / https://biblioclub.ru/index.php?page=book_red&id=429032
6.3. Перечень программного обеспечения	
6.3.1	Microsoft Office;
6.3.2	ПО Лаборатории Касперского в рамках лицензионного соглашения
6.4 Перечень информационных справочных систем	
6.4.1	Консультант +

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения, лабораторными установками. Для проведения лекционных занятий используется демонстрационное оборудование. Лабораторные занятия проводятся в ком-пьютерных классах, рабочие места в которых оборудованы необходимыми лицензионны-ми программными средствами и выходом в Интернет

8. МЕТОДИЧЕСТКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)
Методические указания по освоению дисциплины представлены в Приложении 1 к рабочей программе дисциплины.

Приложение 1
к рабочей программе

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры
Информационные технологии и защита
информации
Протокол № 10 от 11 мая 2018 г.
Зав.кафедрой _____ *Тищенко Е.Н.*

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Компьютерная вирусология
(наименование дисциплины)

10.03.01 Информационная безопасность

10.03.01.02 Организация и технология защиты информации

Уровень образования
Бакалавриат

Составитель _____ Шейдаков Н.Е., доцент каф. ИТиЗИ, к.ф.-м.н., доцент
(подпись) *Ф.И.О., должность, ученая степень, ученое звание*

Ростов-на-Дону, 2018

Оглавление

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Перечень компетенций с указанием этапов их формирования представлен в п. 3. «Требования к результатам освоения дисциплины» рабочей программы дисциплины.

2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

2.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации			
З.: сущность предмета компьютерной вирусологии; методы	*поиск и сбор необходимой литературы, использование современных информационно- коммуникационных технологий и глобальных информационных ресурсов*	*соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации*	*О – опрос (вопрос 1), ЛР –л работа, Р – реферат,*
У.: обнаруживать и удалять компьютерные вирусы и другие вредоносные программы	*выполнение лабораторных экспериментов по тематике курса*	*объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к лабораторной работе*	*О – опрос (вопрос 2) ЛР – лабораторная работа*
В.: методами и средствами защиты от компьютерных вирусов	*выполнение лабораторных экспериментов по тематике курса*	*объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к лабораторной работе*	*О – опрос (вопрос 2) ЛР – лабораторная работа*

2.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

для экзамена:
84-100 баллов (оценка «отлично»)
67-83 баллов (оценка «хорошо»)
50-66 баллов (оценка «удовлетворительно»)
0-49 баллов (оценка «неудовлетворительно»)

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Раздел 1 Основные понятия о компьютерных вирусах……
О 1. (письменный опрос №1)

Вопросы для контрольного письменного опроса
1. Теоретические вопросы

1. Как назывался один из первых вирусов современного типа?
a) The Greeper
b) The Rabbit
c) никак

2. Увеличение температуры процессора - признак заражения?
a) да
b) нет
c) иногда

4. Какова основная особенность компьютерных вирусов?
a) распространение через Интернет
b) выполнение вредоносных действий
c) способность к размножению

3. Сколько существует подходов к классификации вирусов?
a) 1
b) 2

4. Если вирус оставляет в ОП свои части неспособные к размножению, является ли он резидентным?
a) да
b) нет
c) смотря по обстоятельствам

5. Во сколько обошлось Американскому правительству 2 ноября 1988 года?

a) в 100 тыс. долларов
b) в 100 млн. долларов
c) в 0 долларов

6. Легко ли распознать начало заражения?
a) да
b) нет
c) иногда

7. Существует ли строгая последовательность действий при заражении?
a) да
b) нет
c) существует общий набор рекомендаций

8. Какова дата рождения первого вируса?
a) 2 ноября 1988 года
b) 5 сентября 1970 года
c) точной даты не известно

Критерии оценивания:
- оценка «зачтено» выставляется, если ответы даны на все вопросы
- оценка «не зачтено» выставляется, если ответы не даны на все вопросы

Раздел 2 Методы защиты от программ деструктивного воздействия

О 2. (письменный опрос №2)

Вопросы для контрольного письменного опроса

1. Теоретические вопросы

1. Что означает термин "файловые вирусы"?
a) поражают исполняемые файлы
b) оформлены в виде файлов
c) просто так назвали

2. Каков номер статьи УК РФ "Нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети"?
a) 200
b) 274
c) 272

3. Всегда ли симптомы заражения вызваны именно вирусом?
a) да
b) нет
c) никогда

4. Увеличивается ли количество компьютерных вирусов?
a) да
b) нет
c) науке это не известно

5. Самопроизвольное изменение размера файлов - признак заражения?
a) да

b) нет
c) иногда

6. Только ли создание вредоносных программ запрещает статья №273 УК РФ?
a) да
b) нет
c) она вообще этого не запрещает

7. Создатель какого вируса был арестован 18 сентября 2002 года?
a) The Greeper
b) The Rabbit
c) Чернобыль

8. За счёт чего достигается полиморфизм вирусов?
a) за счёт шифрования тела вируса и модификаций программы-расшифровщика
b) за счёт перемешивания его команд
c) за счёт удаления некоторых команд

9. Всегда ли заметно заражение вирусом по работе компьютера?
a) да
b) нет
c) никогда

10. Какое событие произошло 2 ноября 1988 года?
a) появился первый полиморфный вирус
b) упала вся компьютерная сеть США
c) появился первый хакер

Критерии оценивания:

- оценка «зачтено» выставляется, если ответы даны на все вопросы
- оценка «не зачтено»выставляется, если ответы не даны на все вопросы

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра **Информационных технологий и защиты информации**
(наименование кафедры)

Вопросы к экзамену

по дисциплине **Компьютерная вирусология**
(наименование дисциплины)

1. Компьютерные вирусы. Основные определения.
2. Классификация компьютерных вирусов.
3. Обзор способов заражения компьютерных систем и сетей.
4. Макровирусы.
5. Основные принципы полиморфизма на примере макровирусов.

6. Почтовые черви.
7. Троянские программы. Общие принципы работы. Типы троянских программ.
8. Троянские программы типа Backdoor, алгоритм, структура.
9. Вирусы, поражающие com-файлы.
10. Вирусы, поражающие exe-файлы MS DOS.
11. Загрузочные (boot) вирусы.
12. Резидентные вирусы в системе MS DOS.
13. Полиморфные вирусы.
14. Stealth-вирусы.
15. Вирусы, работающие в системе Windows XP/7/2003/2008, принципы работы.
16. Методы борьбы с вирусами.
17. Антивирусные программы. Типы, примеры.
18. Антивирусные комплексы. AVP. DrWeb. EsetNod32
19. Выбор антивирусного программного средства.
20. Принципы организации антивирусной защиты предприятия.
21. Правовые аспекты компьютерной вирусологии

Составитель _____ Шейдаков Н.Е.
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра **Информационных технологий и защиты информации**

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

по дисциплине **Компьютерная вирусология**

1. Компьютерные вирусы. Основные определения
2. Каковы признаки заражения системы?

Составитель Н.Е. Шейдаков
(подпись)

Заведующий кафедрой

_____ Е.Н. Тищенко
(подпись)

«____»_____20 г.

Примечание * Практическая(ое) задача/задание включается по усмотрению преподавателя.

К комплекту экзаменационных билетов прилагаются разработанные преподавателем и утвержденные на заседании кафедры критерии оценивания по дисциплине.

Критерии оценивания:

- оценка «отлично» (84-100 баллов) выставляется, если изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- оценка хорошо» (67-83 баллов) – наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, студент усвоил основную литературу, рекомендованную в рабочей программе дисциплины;
- оценка «удовлетворительно» (50-66 баллов) – наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;
- оценка неудовлетворительно» (0-49 баллов) ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы».

Оформление тем рефератов (докладов, сообщений)

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра *Информационных технологий и защиты информации*

Темы рефератов (докладов, сообщений)

по дисциплине *Компьютерная вирусология*

1. Антивирус AVG
2. ESET NOD32 Internet Security 10
3. Обзор McAfee Internet Security (2016)
4. Антивирус Avast
5. Отечественная программа DrWeb
6. Panda (Panda Cloud Antivirus)

7. Avira Free Antivirus
8. Kaspersky Internet Security
9. Brain — первый вирус для IBM PC
10. Макровирусы
11. Почтовые черви
12. Вирусы, поражающие com-файлы
13. Вирусы, поражающие exe-файлы
14. Загрузочные вирусы
15. Полиморфные и Stealth-вирусы
16. Вирусы, работающие в среде Windows
17. Методы защиты от компьютерных вирусов
18. Антивирусное программное обеспечение
19. Антивирусная защита мобильных пользователей
20. Логические бомбы
21. Программы Дозвона
22. Сетевые черви и защита от них
23. Троянские программы и защита от них

Методические рекомендации по написанию, требования к оформлению

Содержание работы должно представлять обзор, анализ и обобщение материалов собранных из литературных источников сети Интернет, оформленных в соответствии с требованиями ГОСТ.

Критерии оценки:

- оценка «зачтено» выставляется студенту, *если работа соответствует полноте и содержательности проблемы исследования;, объем выполненных работы в полном объеме); соответствует требованиям по оформлению документа*
- оценка «не зачтено», *…если не выполнено одно из требований.*

Составитель _____ Н.Е. Шейдаков
(подпись)

«____»_____20 г.

Оформление лабораторных работ

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра *Информационных технологий и защиты информации*
(наименование кафедры)

Лабораторные работы

по дисциплине *Компьютерная вирусология*
(наименование дисциплины)

1.Тематика лабораторных работ по разделам и темам

Раздел 1 Основные понятия о компьютерных вирусах……
Лабораторная работа 1. Разработка нерезидентной вирусной EXE-программы
Лабораторная работа 2 Разработка резидентной вирусной EXE-программы
Лабораторная работа 3 Основные признаки присутствия вредоносных программ и методы по устранению последствий вирусных заражений

Раздел 2 Методы защиты от программ деструктивного воздействия
Лабораторная работа 1. Антивирус Касперского 6.0 для Windows Workstations. Локальная установка и управление
Лабораторная работа 2. Антивирус Касперского 5.5 для MS Exchange Server. Установка, настройка, управление
Лабораторная работа 3 Kaspersky Administration Kit. Особенности работы с иерархической структурой Серверов администрирования
Лабораторная работа 4. Подготовка лабораторного стенда - корпоративной сети под управлением ОС Microsoft Windows Server 2016 Standard
Лабораторная работа 5. Развертывание антивирусной защиты в сети лабораторного стенда и управление задачами обеспечения антивирусной защиты на базе комплекса управления защитой Kaspersky Security Center 10 и антивируса Kaspersky Endpoint Security 10
Лабораторная работа 6. Подбор и развертывание сертифицированного решения для удаленного управления антивирусной защитой в корпоративной информационной сети из линейки продуктов Dr.Web Enterprise Security Suite

2. Методические рекомендации по выполнению лабораторных работ

При подготовке к лабораторным занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной работы;
- подготовить ответы на контрольные вопросы, помещённые в конце описания лабораторной работы.

3. Критерии оценки:

- оценка «отлично» выставляется студенту, если . задание выполнено в полном объеме; сделан письменный вывод по заданию в полном объеме;
- оценка «хорошо». задание выполнено в объеме до 70 %; сделан письменный вывод по заданию в объеме до 70%;
- оценка «удовлетворительно» задание выполнено в объеме до 50%; сделан письменный вывод по заданию в объеме до 50%;
- оценка «неудовлетворительно» задание выполнено в объеме менее 50 % сделан письменный вывод по заданию в объеме менее 50%

Составитель _____ Н.Е. Шейдаков
(подпись)

«____»_____20 г.

4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 3 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация экзамена

Экзамен проводится по расписанию экзаменационной сессии в письменном виде. Количество вопросов в экзаменационном задании – 2

. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2
к рабочей программе

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры
Информационных технологий и защиты информации
Протокол № 10 от 11 мая 2018 г..
Зав.кафедрой _____ Тищенко Е.Н.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Компьютерная вирусология
(наименование дисциплины)

10.03.01 Информационная безопасность

10.03.01.02 Организация и технология защиты информации

Уровень образования
Бакалавриат

Составитель _____ Шейдаков Н.Е., доцент каф. ИТиЗИ, к.ф.-м.н., доцент.
(подпись) *Ф.И.О., должность, ученая степень, ученое звание*

Ростов-на-Дону, 2018

Методические указания по освоению дисциплины «Компьютерная вирусология» адресованы студентам очной формы обучения.

Учебным планом по направлению подготовки «Информационная безопасность» предусмотрены следующие виды занятий:

- лекции;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются основные понятия и методы компьютерной вирусологии, даются рекомендации для самостоятельной работы и подготовке к практическим занятиям.

При подготовке к лабораторным занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной работы;
- подготовить ответы на контрольные вопросы, помещённые в конце описания лабораторной работы.

Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой дисциплины «Компьютерная вирусология» осуществляется в ходе занятий методом устного опроса, проверки выполненных индивидуальных заданий, контрольных работ, проверки подготовленных конспектов по выделенным для самостоятельного изучения темам дисциплины. В ходе самостоятельной работы каждый студент обязан прочитать основную и, по возможности, дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных, выделить непонятные термины и найти их значение в энциклопедических словарях.

При реализации различных видов учебной работы используются разнообразные (в т.ч. интерактивные) методы обучения, в частности:

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронной библиотекой ВУЗаhttp://library.rsue.ru/ . Также обучающиеся могут взять на дом необходимую литературу на абонементе вузовской библиотеки или воспользоваться читальными залами вуза.