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

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Компьютерная вирусология

Направление 10.03.01 "Информационная безопасность"
Направленность 10.03.01.02 Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Для набора 2023 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	48	48	48	48
Итого ауд.	80	80	80	80
Контактная работа	80	80	80	80
Сам. работа	28	28	28	28
Часы на контроль	36	36	36	36
Итого	144	144	144	144

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

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

Зав. кафедрой: к.э.н., доцент Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	ознакомление обучаемых с основными понятиями компьютерной вирусологии, и подготовка их к организации защиты компьютерных систем и сетей от компьютерных вирусов

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-1: способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и защищенных технических средств обработки информации

В результате освоения дисциплины обучающийся должен:
Знать:
сущность предмета компьютерной вирусологии; методы диагностики и защиты от компьютерных атак (соотнесено с индикатором ПК-1.1)
Уметь:
обнаруживать и удалять компьютерные вирусы и другие вредоносные программы (соотнесено с индикатором ПК-1.2)
Владеть:
методами и средствами защиты от компьютерных вирусов (соотнесено с индикатором ПК-1.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основные понятия о компьютерных вирусах

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
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 разработки, возникновение эпидемий компьютерных вирусов. / Лек /	6	2	ПК-1	Л1.1, Л1.2, Л1.3, Л1.4, Л2.2, Л2.7
1.2	Тема 1.2.Лекция 2. Теоретические сведения о компьютерных вирусах Введение. Результат Фреда Коэна. Результат Д. Чесса и С. Вайта. Формализм Ф. Лейтольда. Результат Леонарда Адельмана / Лек /	6	2	ПК-1	Л1.1, Л1.2, Л1.4, Л2.3, Л2.7
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, Л1.2, Л1.3, Л1.4, Л2.2, Л2.5, Л2.7
1.4	Тема 1.3. Основные признаки присутствия вредоносных программ и методы по устранению последствий вирусных заражений. Использование Диспетчера задач ОС для анализа подозрительных процессов. Анализ статистку текущих сетевых подключений компьютера с параметрами подключений портов / Лаб /	6	2	ПК-1	Л1.1, Л1.2, Л1.4, Л1.5, Л2.6, Л2.7
1.5	Тема 1.3. "Антивирус ClamAV" Установка ClamAV. Настройка обновления. Сканирование системы с помощью ClamAV.Установка ClamTk (графический пользовательский интерфейс для ClamAV) / База знаний РЕД ОС / Лаб /	6	2	ПК-1	Л1.1, Л1.3, Л2.1, Л2.7
1.6	Тема 1.4. Установка Kaspersky для Linux. Изучение руководства по использованию. Инсталяция дистрибутива программы. Установка Агента администрирования. Начальная настройка параметров Агента администрирования. Тестирование программы. / ПО Лаборатории Касперского. РЭД ОС LibreOffice / Лаб /	6	4	ПК-1	Л1.1, Л1.2, Л1.4, Л2.6, Л2.7
1.7	Тема 1.3. «ЗАРАЖЕНИЕ COM-файлов»	6	4	ПК-1	Л1.1, Л1.2, Л1.3,

	Изучение структуры файла программы вируса, способов её загрузки и воздействия на COM-файлы на примере тестовой программы вируса. Его обнаружение и нейтрализация с помощью антивирусного комплекса. / ПО лаборатории Касперского. РЭД ОС LibreOffice / Лаб /				Л1.5, Л2.1, Л2.7
1.8	Тема 1.3. «ЗАРАЖЕНИЕ EXE-файлов» Изучение структуры файла программы вируса, способов её загрузки и воздействия на EXE-файлы на примере тестовой программы вируса. Его обнаружение и нейтрализация с помощью антивирусного комплекса./ ПО лаборатории Касперского. РЭД ОС LibreOffice / Лаб /	6	4	ПК-1	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.7
1.9	Тема 1.4. «Файловые вирусы» Ознакомление со способами организации заражения файлов. Изучение структуры файла программы вируса, способов её загрузки и воздействия на COM-файлы на примере тестовой программы вируса. Его обнаружение и нейтрализация с помощью антивирусного комплекса. / ПО Лаборатории Касперского. РЭД ОС LibreOffice / Лаб /	6	4	ПК-1	Л1.1, Л1.2, Л1.4, Л2.6, Л2.7
1.10	Тема 1.3. «Основные определения. Классификация» Файловые вирусы DOS Классификация по способу использования ресурсов. Классификация по типу заражаемых объектов. Классификация по принципам активации. Классификация по способу организации программного кода. Функционированиея вирусов -«спутников» (вирусы-«компаньоны»). Оверлейные» вирусы. Нерезидентные вирусы. Резидентные вирусы Вирусы -«невидимки». / Ср /	6	2	ПК-1	Л1.1, Л1.2, Л1.4, Л2.2, Л2.7
1.11	Тема 1.3. «Основные определения. Классификация» Загрузочные вирусы Згрузка с винчестера. Как устроены загрузочные вирусы. Как загрузочные вирусы получают управление. Как загрузочные вирусы заражают свои жертвы. Как вирусы остаются резидентно в памяти. / Ср /	6	2	ПК-1	Л1.1, Л1.2, Л1.4, Л2.3, Л2.7
1.12	Тема 1.4. «Файловые вирусы» Технологии заражения «Стандартный» метод заражения. Заражение в середину файла. Заражение в начало файла. Метод предопределенного местоположения файлов. Метод поиска в текущем каталоге. Метод рекурсивного обхода дерева каталогов. Способы выделения вирусом фрагмента памяти. Обработка прерываний. Перехват запуска программы. Перехват файловых операций / Ср /	6	6	ПК-1	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.7

Раздел 2. Методы защиты от программ деструктивного воздействия

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
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, Л1.2, Л1.4, Л2.3, Л2.4, Л2.5, Л2.7
2.2	Тема 2.2. «Защита шлюзов»: Общие сведения. Возможные схемы защиты. Требования к антивирусам для шлюзов. Угрозы и методы защиты от них. Эксплуатационные характеристики. / Лек /	6	4	ПК-1	Л1.1, Л1.2, Л1.4, Л1.5, Л2.4, Л2.7
2.3	Тема 2.3. «Защита почтовых систем» Общие сведения. Возможные схемы защиты. Требования к антивирусному комплексу для проверки почтового потока. Unix-системы. / Лек /	6	4	ПК-1	Л1.1, Л1.2, Л1.4, Л1.5, Л2.4, Л2.7
2.4	Тема 2.3.1. Лекция. Назначение средств защиты почтовых систем Защита компьютеров пользователей от опасных программ, распространяющихся через почту. Интегрирование средств защиты с почтовой системой. Построения комплексной системы антивирусной защиты (КСАЗ). / Лек /	6	4	ПК-1	Л1.1, Л1.2, Л1.4, Л2.7
2.5	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, Л1.4, Л1.5, Л2.4, Л2.6, Л2.7
2.6	Тема 2.5 "Компьютерные атаки и технологии их обнаружения" Описаны угрозы безопасности информации и	6	4	ПК-1	Л1.1, Л1.2, Л1.3, Л1.4, Л2.5, Л2.6,

	способы их реализации, ущерб, приносимый вредоносными программами в результате их действия. / Лек /				Л2.7
2.7	Тема 2.1. «Антивирус Касперского для Linux" Ознакомление с процессом инсталляции, принципами работы и управления Антивирусом Касперского / По Касперского. РЭД ОС LibreOffice. / Лаб /	6	4	ПК-1	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.7
2.8	Тема 2.1. "Межсетевой экран (firewall)" ознакомиться с различными типами межсетевых экранов и теорией их построения; изучить работу Outpost Firewall Pro межсетевого экрана для систем Linux. Инсталяция и настроить Outpost Firewall Pro. /РЭД ОС LibreOffice, свободно распространяемое ПО Outpost Firewall Pro / Лаб /	6	4	ПК-1	Л1.1, Л1.3, Л2.1, Л2.7
2.9	Тема 2.3. «Защита почтовых систем» Ознакомиться с процессом инсталляции, принципами работы и управления Антивирусом Касперского 5.5 / По Касперского. РЭД ОС LibreOffice. / Лаб /	6	4	ПК-1	Л1.1, Л1.2, Л1.4, Л2.6, Л2.7
2.10	Тема 2.4. «Защита серверов и рабочих станций» Антивирусный комплекс Kaspersky Administration Kit По Касперского. Ознакомление с процессом инсталляции, принципами работы Kaspersky Administration Kit и способами построения логической сети, задачами удаленной установки и обновления приложений в среде РЕД ОС. / ПО лаборатории Касперского.РЭД ОС LibreOffice. / Лаб /	6	6	ПК-1	Л1.1, Л1.2, Л1.4, Л2.6, Л2.7
2.11	Тема 2.4. «Защита серверов и рабочих станций». Kaspersky Endpoint Security 11 для Linux Ознакомление с процессом инсталляции, принципами работы Kaspersky Administration Kit и способами построения логической сети, задачами удаленной установки и обновления приложений в среде ОС Linux. / ПО лаборатории Касперского.РЭД ОС LibreOffice. /ПО лаборатории Касперского, РЭД ОС LibreJffice/ / Лаб /	6	6	ПК-1	Л1.1, Л1.2, Л1.4, Л2.1, Л2.7
2.12	Тема 2.5. Пример написания антивируса Ознакомление с методикой разработки и написания тестового вируса на языке программирования С++, способами организации заражения файловой структуры в среде ОС Linux. / ПО Лаборатории Касперского. РЭД ОС LibreOffice / Лаб /	6	4	ПК-1	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1
2.13	Тема 2.1. «Что такое антивирусы». Мобильные антивирусы: защита планшетов и телефонов Технология - MDM (Mobile Device Management), управление мобильными устройствами. концепция BYOD – Bring Your Own Device («приноси собственное устройство». COPE – Corporate – Owned, Personally Enabled («корпоративные устройства, настройкой и обслуживанием которых сотрудник занимается самостоятельно»). / Ср /	6	4	ПК-1	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.7
2.14	Тема 2.1. «Что такое антивирусы». Антивирусный комплекс DoctorWeb Dr.Web — общее название семейства антивирусного ПО для различных платформ и линейки программно-аппаратных решений (Dr.Web Office Shield, а также решений для обеспечения безопасности всех узлов корпоративной сети (Dr.Web Enterprise Suite[2]). Разрабатывается компанией «Доктор Веб». Продукты предоставляют защиту от вирусов, троянского, шпионского и рекламного ПО, червей, руткитов, хакерских утилит, программ-шуток, а также неизвестных угроз с помощью различных технологий реального времени и поведенческого анализа. / Ср /	6	4	ПК-1	Л1.1, Л1.2, Л1.4, Л2.1, Л2.7
2.15	Тема 2.1. «Что такое антивирусы». Антивирусный комплекс ESET Nod32 ESET NOD32 — комплексное антивирусное решение для защиты в реальном времени. ESET NOD32 обеспечивает защиту от вирусов, а также от других угроз, включая троянские программы, черви, spyware, adware, фишинг-атаки. В ESET NOD32 используется патентованная технология ThreatSense, предназначенная для выявления новых возникающих угроз в реальном времени путём анализа выполняемых программ на наличие вредоносного кода, что позволяет предупреждать действия авторов вредоносных программ. / Ср /	6	4	ПК-1	Л1.1, Л1.2, Л1.4, Л2.1, Л2.7
2.16	Тема 2.5 «Экономические и правовые аспекты компьютерной вирусологии»	6	6	ПК-1	Л1.1, Л1.2, Л1.4, Л2.1, Л2.7

	Уголовное и административное преследование за создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно распространение таких программ или машинных носителей с такими программами / Ср /				
2.17	/ Экзамен /	6	36	ПК-1	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6, Л2.7

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Михайлов А. В.	Компьютерные вирусы и борьба с ними: практическое пособие	Москва: Диалог-МИФИ, 2012	https://biblioclub.ru/index.php?page=book&id=136089 неограниченный доступ для зарегистрированных пользователей
Л1.2	Положевец Г.	БИТ. Бизнес & Информационные технологии: бизнес & информационные технологии: журнал	Москва: Синдикат 13, 2012	https://biblioclub.ru/index.php?page=book&id=136953 неограниченный доступ для зарегистрированных пользователей
Л1.3		Вирусы и средства борьбы с ними: курс: учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2007	https://biblioclub.ru/index.php?page=book&id=234893 неограниченный доступ для зарегистрированных пользователей
Л1.4	Аверченков, В. И., Рытов, М. Ю.	Организационная защита информации: учебное пособие для вузов	Брянск: Брянский государственный технический университет, 2012	https://www.iprbookshop.ru/7002.html неограниченный доступ для зарегистрированных пользователей
Л1.5	Касперски К	Компьютерные вирусы изнутри и снаружи	Санкт-Петербург: Питер, 2010	https://ibooks.ru/reading.php?short=1&productid=21495 неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Положевец Г.	БИТ. Бизнес & Информационные технологии: бизнес & информационные технологии: журнал	Москва: Синдикат 13, 2012	https://biblioclub.ru/index.php?page=book&id=136948 неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.2	Яшутина О. А.	Обеспечение информационной безопасности с помощью антивируса Касперского. Лекция 1. Классификация вредоносных программ. Методы защиты. Презентация	Москва: Национальный Открытый Университет «ИНТУИТ», 2014	http://biblioclub.ru/index.php?page=book&id=239488 неограниченный доступ для зарегистрированных пользователей
Л2.3	Яшутина О. А.	Обеспечение информационной безопасности с помощью антивируса Касперского. Лекция 2. Локальное использование Антивируса Касперского 6.0. Презентация	Москва: Национальный Открытый Университет «ИНТУИТ», 2014	http://biblioclub.ru/index.php?page=book&id=239491 неограниченный доступ для зарегистрированных пользователей
Л2.4	Яшутина О. А.	Обеспечение информационной безопасности с помощью антивируса Касперского. Лекция 4. Антивирус Касперского для Linux File Server. Презентация	Москва: Национальный Открытый Университет «ИНТУИТ», 2014	http://biblioclub.ru/index.php?page=book&id=239492 неограниченный доступ для зарегистрированных пользователей
Л2.5	Чепурнова Н. М., Ефимова Л. Л.	Правовые основы информатики: учебное пособие	Москва: Юнити-Дана, 2015	https://biblioclub.ru/index.php?page=book&id=426501 неограниченный доступ для зарегистрированных пользователей
Л2.6	Климентьев К. Е.	Компьютерные вирусы и антивирусы: взгляд программиста	Москва: ДМК Пресс, 2013	https://ibooks.ru/reading.php?short=1&productid=344099 неограниченный доступ для зарегистрированных пользователей
Л2.7	Башлы, П. Н., Бабаш, А. В., Баранова, Е. К.	Информационная безопасность и защита информации: учебное пособие	Москва: Евразийский открытый институт, 2012	https://www.iprbookshop.ru/10677.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

СПС КонсультантПлюс
web.Anet https://webanetlabs.net/
ФСТЭК России/fstec.ru
Официальный сайт РЭД ОС edos.red-soft.ru/base/manual/safe-redos/

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
LibreOffice
ПО Лаборатории Касперского

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными программными средствами и выходом в Интернет.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ
Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-1: способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и защищенных технических средств обработки информации			
З.: сущность предмета компьютерной вирусологии; методы диагностики и защиты от компьютерных атак	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	Э (1-60) О (1-14)
У.: обнаруживать и удалять компьютерные вирусы и другие вредоносные программы	выполнение лабораторных экспериментов по установке и настройке антивирусных программ	правильность выполнения заданий, объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к лабораторной работе	ПОЭЗ (5-10) ЛЗ (разд.1 ЛЗ 1-6; разд.2 ЛЗ 7-12)
В.: методами и средствами защиты от компьютерных вирусов	выполнение лабораторных экспериментов по тематике курса	правильность выполнения заданий, объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к лабораторной работе	ПОЭЗ (5-10) ЛЗ (разд.1 ЛЗ 1-6; разд.2 ЛЗ 7-12)

О – опрос, Э. – вопросы к экзамену; ПОЭЗ – практико-ориентированные задания к экзамену; ЛЗ – лабораторные задания

1.2 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»)

2 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

Вопросы к экзамену

1. Компьютерные вирусы. Основные определения.
2. Классификация компьютерных вирусов.
3. Обзор способов заражения компьютерных систем и сетей.
4. Макровирусы.
5. Назначение средств защиты почтовых систем
6. Защита почтовых систем
7. Основные принципы полиморфизма на примере макровирусов.
8. Почтовые черви.
9. Троянские программы. Общие принципы работы. Типы троянских программ.

10. Троянские программы типа Backdoor, алгоритм, структура.
11. Вирусы, поражающие com-файлы.
12. Вирусы, поражающие exe-файлы MS DOS.
13. Загрузочные (boot) вирусы.
14. Резидентные вирусы в системе MS DOS.
15. Полиморфные вирусы.
16. Stealth-вирусы.
17. Вирусы, работающие в системе Windows, принципы работы.
18. Методы борьбы с вирусами.
19. Антивирусные программы. Типы, примеры.
20. Антивирусные комплексы. AVP. DrWeb. EsetNod32
21. Выбор антивирусного программного средства.
22. Принципы организации антивирусной защиты предприятия.
23. Защита шлюзов.
24. Защита серверов и рабочих станций
25. Правовые аспекты компьютерной вирусологии
26. Какова основная особенность компьютерных вирусов? Дайте понятие вируса.
27. Когда были отмечены первые появления вирусов?
28. Сколько существует подходов к классификации вирусов? Перечислите их.
29. Что означает термин "файловые вирусы"?
30. Что означает термин "загрузочные вирусы"?
31. Что означает термин "сетевые вирусы"?
32. Что означает термин "макровирусы"?
33. Что означает термин "flash - вирусы"?
34. Что означает термин "резидентные вирусы"?
35. Что означает термин "нерезидентные вирусы"?
36. Что означает термин "безвредные вирусы"?
37. Что означает термин "неопасные вирусы"?
38. Что означает термин "опасные вирусы"?
39. Что означает термин "очень опасные вирусы"?
40. Что означает термин "вирусы - спутники"?
41. Что означает термин "черви"?
42. Что означает термин "паразитические вирусы"?
43. Что означает термин "стелс - вирусы"?
44. Что означает термин "полиморфные вирусы"?
45. Что означает термин "макровирусы"(в связи с особенностями алгоритма работы)?
46. Какие макровирусы сейчас наиболее распространены?
47. Как распространяются "черви"?
48. За счёт чего достигается полиморфизм вирусов?
49. Всегда ли заметно заражение вирусом по работе компьютера?
50. Каковы признаки заражения системы?
51. Существует ли строгая последовательность действий при заражении?
52. Нужно ли как то ограничивать доступ к носителям с этой информацией?
53. Перечислите основные методы профилактики заражения?
54. Приведите примеры наиболее известных антивирусов?
55. Как называется статья №272 УК РФ?
56. Как называется статья №273 УК РФ?
57. Как называется статья №274 УК РФ?
58. Как наказывается неправомерный доступ к компьютерной информации?
59. Что означает термин "вредоносная программа"?
60. Как наказывается создание вредоносных программ, повлекшее по неосторожности тяжкие последствия?

Практико-ориентированные задания к экзамену

1. Порядок запуска почтового клиента на рабочей стации и файловом сервере обмена тестовыми почтовыми сообщениями и проверка в работоспособности Linux Mail Server и почтовых клиентов.
2. Произвести настройки Сервера безопасности доступными по гиперссылке Перечислите модули системы и доступные им уровни диагностики, запишите название защищаемого хранилища почтовых ящиков и название защищаемого хранилища общих папок.
3. Настройка и активация получения уведомлений о зараженном объекте, чтобы почтовое уведомление приходило получателю и отправителю, а сообщение NET SEND приходило на рабочую станцию.
4. Порядок тестирования Доверенной зоны, отключение Сетевых дисков в Файловом антивирусе и внесение папку c:\test_virus в Доверенную зону.
5. Включите Мониторинг системного реестра, и проверьте работу правил, отвечающих за автоматический запуск программ при загрузке операционной системы.
6. В глобальном контейнере Задачи, создайте задачу Установка агента, предназначенную для установки Агента администрирования на рабочую станцию.
7. Создайте инсталляционный пакет Kaspersky Endpoint Security для Linux**.**
8. Настройте параметры обновления антивирусных баз Антивируса Касперского для Linux File Server на получение обновлений из указанного преподавателем источника. Произведите обновление антивирусных баз.
9. Какие каталоги первого уровня содержит файловая система РЕД ОС?
10. Проанализируйте файл system.ini на предмет подозрительных записей. При необходимости внесите корректировки в файл system.ini.

Критерии оценивания:

- 84-100 (оценка «отлично») –баллов (оценка «отлично») - 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;
- 67-83 (оценка «хорошо») – баллов (оценка «хорошо») - 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, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;
- 50-66 (оценка «удовлетворительно») –баллов (оценка удовлетворительно) - 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;
- 0-49 (оценка «неудовлетворительно») –баллов (оценка неудовлетворительно) - 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.

Перечень теоретических вопросов для опроса

1. Каким образом буду проверяться архивы при отключенном механизме распаковки архивов в Антивирусе Касперского для Microsoft ISA Server?
2. Какие варианты установки лицензионного ключа существуют в Антивирусе Касперского 6.0 для Linux Workstations?
3. Объясните принципы работы компонента Анти-Хакер.
4. Какое количество резервных копий антивирусных баз сохраняется в Антивирусе Касперского 6.0 для Linux Workstations?
5. Какие типы архивов проверяются Файловым антивирусом?
6. Какие модули содержит компонент Анти-Шпион? Какого их назначение?
7. Какие протоколы поддерживаются Почтовым антивирусом?

8. Для чего предназначена папка общего доступа Share, которая создается в процессе установки Сервера администрирования?

9. Какие порты использует Сервер администрирования для связи с Агентами администрирования?

10. Какое различие между глобальной и групповой задачей удаленной установки Агента администрирования?

11. Какие две основные технологии обновления антивирусных баз существуют, в чем их отличие?

12. Каким образом можно изменять настройки унаследованной политики?

13. Какие способы применения политик на клиентских компьютерах существуют в Kaspersky Administration Kit? В чем различие этих способов?

14. Объясните в чем отличие понятий вирус и вредоносная программа.

Примечание: опрос проводится при проверке всех лабораторных заданий для выявления знаний при изучении соответствующих тем дисциплины в рамках текущей аттестации.

Критерии оценивания:

- 2 балла выставляется обучающемуся, если изложенный материал фактически верен и логически обоснован.
- 1 балл выставляется обучающемуся, если изложенный материал фактически верен, но есть незначительные ошибки.
- 0 баллов, если ответ не верен

Максимальное количество баллов за семестр – 28 баллов.

Лабораторные задания

Тематика лабораторных работ по разделам и темам

Раздел 1 Основные понятия о компьютерных вирусах

Лабораторное задание 1. Основные признаки присутствия вредоносных программ и методы по устранению последствий вирусных заражений (6 баллов)

1. Запуск Диспетчер задач ОС и анализ запущенных процессов
2. Используя Диспетчер задач выгрузить подозрительные процессы.
3. Запустите интерфейс командной строки. Ознакомьтесь с ключами команды netstat.
4. Запустите утилиту работы с реестром.
5. Проанализируйте файл system.ini
6. Используя стандартные средства поиска, найти файлы, которые порождали подозрительные процессы и удалить их.

Лабораторное задание 2. Антивирус ClamAV. (6 баллов)

1. Установка ClamAV.
2. Настройка обновления.
3. Сканирование системы с помощью ClamAV.
4. Установка ClamTk

Лабораторное задание 3. Установка Kaspersky для Linux. (6 баллов)

1. Аппаратные требования
2. Дистрибутивы
3. Установка программы.
4. Проверка актуальности лицензии
5. Установка Агента администрирования
6. Начальная настройка параметров Агента администрирования

Лабораторное задание 4. Разработка резидентной вирусной COM-программы (6 баллов)

1. Изучение структуры вируса на основе описания листинга программы.
2. Набор текста программы в редакторе Ассемблер
3. Отладка текста программы.
4. Трансляция программы в objeck-файл
5. Запуск программы и обнаружение заражения.

Лабораторное задание 5. Разработка нерезидентной вирусной EXE-программы (6 баллов)

1. Изучение структуры вируса на основе описания листинга программы.

2. Набор текста программы в редакторе Ассемблер
3. Отладка текста программы.
4. Трансляция программы в object-файл
5. Запуск программы и обнаружение заражения.
Лабораторное задание 6. Файловые вирусы в Linux. (6 баллов)
1. Ознакомление со способами организации заражения файлов в среде ОС Linux.
2. Набор текста программы в редакторе Ассемблер
3. Отладка текста программы.
4. Трансляция программы в object-файл
5. Запуск программы и обнаружение заражения.
Раздел 2 Методы защиты от программ деструктивного воздействия
Лабораторное задание 7. Антивирус Касперского для Linux File Server. Установка, настройка, управление (6 баллов)
1. Изучить процесс установки Антивируса Касперского для Linux File Server
2. Ознакомиться с назначением и функциями Антивируса Касперского
3. Ознакомиться с возможностями управления Антивирусом Касперского для Linux File Server через консоль Management
4. Выполнить задания к лабораторной работе
5. Защитить лабораторную работу, ответив на контрольные вопросы
Лабораторное задание 8 Межсетевой экран (firewall) (6 баллов)
1. Настройка сетевых соединений (настроить политики безопасности; настроить локальную сеть).
2. Предотвращение сетевых атак: настроить уровень обнаружения атак; настроить защиту от Ethernet-атак;
настроить сканер портов.
3. Наблюдение за сетевой активностью: проанализировать сетевую активность; проанализировать список используемых портов.
4. Защита от вредоносного ПО: настройка графика проверки системы; настройка постоянной защиты от вредоносных программ; настройки сканирования почтовых вложений.
5. Контроль веб-активности: настроить уровни веб-контроля; настройка блокировщика рекламы; настроить блокировщик шпионских сайтов.
Лабораторное задание 9. Kaspersky Administration Kit. Особенности работы с иерархической структурой Серверов администрирования (6 баллов)
1. Ознакомиться с процессом подключения и управления *подчиненным Сервером* администрирования
2. Ознакомиться с процессом создания политик и задач, правилами их наследования
3. Ознакомиться с видами отчетов и событий в Kaspersky Administration Kit
4. Ознакомиться с работой утилиты резервного копирования
5. Выполнить задания к лабораторной работе
6. Защитить лабораторную работу, ответив на контрольные вопросы
Лабораторное задание 10. Kaspersky Endpoint Security 11 для Linux (6 баллов)
1. Изучить процесс установки Касперского для Linux Workstations
2. Ознакомиться с составом и функциями Касперского для Linux Workstations
3. Ознакомиться со структурной схемой, элементами и объектами управления логической сети
4. Ознакомиться с возможностями создания и работой задач удаленной
установки антивирусного программного обеспечения
5. Ознакомиться с возможностями создания и работой задач обновления антивирусных баз Сервера администрирования и Антивируса Касперского для Linux Workstations
6. Ознакомиться с настройками и работой задачи Смена Сервера администрирования
7. Защитить лабораторную работу, ответив на контрольные вопросы
Лабораторное задание 11. Защита почтовых систем (6 баллов)
1. Изучить процесс установки Антивируса Kaspersky Security для Linux Mail Server
2. Ознакомиться с назначением и функциями Антивируса Касперского для Linux Mail Server
3. Ознакомиться с возможностями управления Антивирусом Касперского для Linux Mail Server
4. Ознакомиться с возможностями управления Антивирусом Касперского для Linux Mail Server через Консоль администрирования

5. Выполнить задания к лабораторной работе
6. Защитить лабораторную работу, ответив на контрольные вопросы
Лабораторное задание 12. Пример написания антивируса (6 баллов)
1. Ознакомление с методикой разработки и написания тестового вируса на языке программирования C++
2. Ознакомление со способами организации заражения файловой структуры в среде ОС Linux.
3. Набор текста программы в редакторе Ассемблер
4. Отладка текста программы.
5. Трансляция программы в object-файл
6. Запуск программы и обнаружение заражения.

Критерии оценивания:

Баллы по каждому заданию проставлены в скобках (6 баллов × 12).

Распределение баллов по заданию:

инсталляция ПО от 0 до 2 баллов; настройка программного продукта от 0 до 2 баллов; тестирование рабочей станции или сети от 0 до 1 баллов; выводы по выполненному заданию от 0 до 1 баллов. Неправильные задания – 0 баллов.

Максимальное количество баллов, которое может получить обучаемый за семестр – **72** балла.

3. 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. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме экзамена.

Экзамен проводится по расписанию экзаменационной сессии в письменном виде. Количество вопросов в экзаменационном задании – 3. 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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом 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 лабораторным.

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, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой дисциплины «Компьютерная вирусология» осуществляется в ходе занятий методом опроса, посредством выполнения лабораторных заданий. 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 библиотечное литературе или на электронных ресурсах.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.