МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

«Утверждаю»
Заведующий кафедрой ТО и ЗИ

А.А. Сирота
«23» 04 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.04 Защита от вредоносных программ

1. Код и наименование направления подготовки / специальности:
10.03.01 Информационная безопасность

2. Профиль подготовки / специализация/магистерская программа:
Безопасность компьютерных систем

3. Квалификация (степень) выпускника:
Бакалавр

4. Форма обучения:
Очная

5. Кафедра, отвечающая за реализацию дисциплины:
Кафедра технологий обработки и защиты информации

6. Составители программы:
Вялых Сергей Ариевич, кандидат технических наук

7. Рекомендована:
протокол НМС ФКН № 5 от 05.03.2024 г.

8. Учебный год: 2027-2028 **Семестр(ы):** 8

9. Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

освоение студентами основных положений теории защиты информации от вредоносных программ и методологии оценки угроз безопасности информации, характерных для современных информационных технологий. Должно быть сформировано представления об основных видах вредоносных программ, их потенциальных возможностях и об угрозах безопасности информации, которые могут быть ими реализованы в компьютерных системах.

Задачи дисциплины:

- освоение студентами положений и требований, современных нормативно-методических документов, регламентирующих меры защиты от вредоносных программ;
- формирование представления об основных видах вредоносных программ, их потенциальных возможностях и об угрозах безопасности информации, которые могут быть ими реализованы в компьютерных системах;
- изучение основных положений теории защиты информации от вредоносных программ;
- формирование представления о приемах и методах исследования возможностей вредоносных программ;
- овладение практическими навыками защиты информационных систем от вредоносных программ.

10. Место учебной дисциплины в структуре ООП:

Входит в часть, формируемую участниками образовательных отношений (вариативная) блока Б1.

Для успешного освоения дисциплины необходимы входные знания в области основ информационной безопасности, организационного и правового обеспечения информационной безопасности, архитектуры информационных систем, навыки программирования.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-1	Способен выполнять работы по проектированию программного обеспечения	ПК-1.3	Умеет применять технологии обработки данных при разработке программного обеспечения в профессиональной деятельности	Знать: положения и требования, современных нормативно-методических документов, регламентирующих меры защиты от вредоносных программ. Уметь: обосновывать решения, связанные с реализацией антивирусных средств защиты информации в пределах должностных обязанностей; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих антивирусную защиту; формулировать основные требования в области антивирусной защиты информации; анализировать и обобщать материалы научно-технической литературы, нормативных и методических материалов по вопросам защиты информации от вредоносных программ. Владеть: практическими навыками использования современных антивирусных средств защиты информации.

ПК-3	Способен осуществлять администрирование антивирусных средств защиты информации и прикладного программного обеспечения, использовать современные технологии защиты объектов электронного контента от несанкционированного использования	ПК-3.1	знает современные технологии защиты электронного документооборота, технологии защиты объектов электронного контента от несанкционированного использования	Знать: основные положения теории защиты информации от вредоносных программ, методы и возможности обнаружения вредоносных программ; задачи развёртывания антивирусной защиты информации на предприятиях; систему организационных мер, направленных на антивирусную защиту информации;
		ПК-3.2	умеет анализировать возможности использования современных технологий защиты данных и объектов электронного контента	Уметь: проводить анализ объектов и систем на соответствие требованиям нормативных документов в области защиты от вредоносных программ; формулировать основные требования, предъявляемые к антивирусной защите информации. Владеть: практическими навыками формирования требований и контроля выполнения требований и мер по антивирусной защите информации; практическими навыками формирования комплексного подхода к обеспечению информационной безопасности объекта защиты.

12. Объем дисциплины в зачетных единицах/час — 2/72.
Форма промежуточной аттестации: *зачет с оценкой.*

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра 8	№ семестра	…
Аудиторные занятия		48	48		
в том числе:	лекции	12	12		
	лабораторные	36	36		
	контроль				
Самостоятельная работа		24	24		
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(зачет с оценкой – __час.)*					
Итого:		72	72		

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Виды вредоносных программ	1. Основные виды вредоносных программ и особенности их функционирования. История вопроса. Классификация компьютерных вирусов. Признаки присутствия на компьютере вредоносных программ.	

1.2	Исследование возможностей наиболее распространенных антивирусных программ	2. Исследование возможностей наиболее распространённых антивирусных программ. Особенности использования программы обнаружения вредоносных программ AVZ. Скрипты и управление AVZ.	
1.3	Теоретические сведения о вредоносных программах	3. Теоретические сведения о компьютерных вирусах. Формальные модели и исследование потенциальных возможностей вредоносных программ. Основные положения теории алгоритмов. Машина Тъюринга. 4. Модели компьютерного вируса, сетевого червя. Оценка потенциальных алгоритмических свойств вредоносных программ. Современные тенденции развития угроз безопасности информации, связанные с применением программного обеспечения.	
1.4	Практические методы и приемы исследования вредоносных программ	5. Практические методы и приемы исследования вредоносных программ. Отладчики и дизассемблеры. Основные возможности отладчиков Soft-Ice, IDA, OllyDbg.	
1.5	Основные технологии разработки и внедрения вредоносных программ	6. Архитектура построения современных вычислительных систем с точки зрения возможностей воздействия вредоносных программ. Возможности низкоуровневого воздействия. Современные тенденции развития угроз безопасности информации, связанные с вредоносными про-граммами.	
1.6	Типовые способы и средства компьютерной разведки	7. Понятие, основные этапы, типовые способы и средства компьютерной разведки. Современные сканеры уязвимостей информационных систем.	
1.7	Основные направления защиты от вредоносных программ	8. Основные направления защиты от вредоносных программ. Средства обнаружения вторжений.	
2. Практические занятия			
2.1	нет		
3. Лабораторные работы			
3.1	Виды вредоносных программ	1. Знакомство с первыми компьютерными вирусами. Вирус 1701 (падающие буквы).	
3.2	Исследование возможностей наиболее распространенных антивирусных программ	2. Исследование основных возможностей антивирусных программ лаборатории Касперского. 3. Исследование программы обнаружения вредоносных программ AVZ. Скрипты и управление AVZ.	
3.3	Теоретические сведения о вредоносных программах	4. Знакомство с полиморфными программными вирусами и генераторами вредоносных программ.	
3.4	Практические методы и приемы исследования вредоносных программ	5. Отладчики и дизассемблеры. Основные возможности отладчиков Soft-Ice, IDA, OllyDbg.	
3.5	Типовые способы и средства компьютерной разведки	6. Исследование возможностей современных сканеров уязвимостей информационных систем. 7. Средства тестирования на проникновение.	
3.6	Основные направления защиты от вредоносных программ	8. Средства обнаружения вторжений.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Сам. работа	Всего
1	Виды вредоносных программ.	1	4	2	7
2	Исследование возможностей наиболее распространенных антивирусных программ	2	4	4	10
3	Теоретические сведения о вредоносных программах.	1	4	2	7

4	Практические методы и приемы исследования вредоносных программ.	2	8	4	14
5	Основные технологии разработки и внедрения вредоносных программ	2	4	2	8
6.	Типовые способы и средства компьютерной разведки	2	8	4	14
7	Основные направления защиты от вредоносных программ.	2	4	6	12
	Итого:	12	36	24	72

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

1) При изучении дисциплины рекомендуется использовать следующие средства:

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;

электронные версии учебников и методических указаний для выполнения лабораторно-практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении лабораторных занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

В ходе самостоятельной работы необходимо уделить основное внимание работе с текстом конспекта лекции, изучению рекомендованной литературы, изучению нормативных документов по информационной безопасности.

4) При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online занятиям, ответственно подходить к заданиям для самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник
1	Монаппа К. А. Анализ вредоносных программ / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2019. – 452 с.
2	Ховард, Майкл. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок : / М. Ховард, Д. Лебланк, Дж. Виега ; авт. предисл. А. Йоран .— Москва : ДМК Пресс, 2009 .— 287 с. : ил. — .— Загл. и авт. ориг.: 19 deadly sins of soft-ware security / Michael Howard, David Leblanc, John Viega .— ISBN 5-9706-0027-X .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1118>.

б) дополнительная литература:

№ п/п	Источник
3	Касперский, Евгений Валентинович. Компьютерное zловредство / Евгений Касперский .— СПб. [и др.] : Питер, 2007 .— 207 с. : ил. + 1 CD https://lib.vsu.ru/zgate?present+4408+default+2+1+F+1.2.840.10003.5.102+rus

4	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors : Обнаружение и защита / О.В. Зайцев. – СПб.: БХВ-Петербург, 2006. - 304 с.
5	Голуб, Владимир Александрович. Защита от вредоносного программного обеспечения: учебное пособие для вузов / В.А. Голуб; Воронеж. гос. ун-т.— Воронеж: ЛОП ВГУ, 2006 .— 31 с. — Библиогр.: с.30 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf>.
6	Мельников, Владимир Павлович. Информационная безопасность и защита информации: учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
7	Пирогов В.Ю. Ассемблер и дизассемблирование / В.Ю. Пирогов. – СПб.: БХВ-Петербург, 2006. - 464 с.
8	Александр Доронин. Бизнес-разведка http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html
9	Вялых А.С. Оценка возможностей атаки на информационную систему / А.С. Вялых, С.А. Вялых // Кибернетика и высокие технологии XXI века : матер. XII международ. науч.-тех. конф., Воронеж, 11-12 мая 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т.1. – С. 91-96.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
10	http://www.z-oleg.com/
11	http://www.kaspersky.ru/
12	Материалы Интернет-Университета Информационных Технологий www.INTUIT.ru
13	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
14	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
15	ЭБС Лань, Лицензионный договор №3010, (с 01/03/2024 по 28.02.2025) 06/02 24 от 13.02.2024 (с дополнительным соглашением №1 от 14.03.2024), ЭБС «Университетская библиотека online» (Контракт №3010 06/11 23 от 26.12.2023 (с 26.12.2023 по 25.12.2024), ЭБС «Консультант студента» – Лицензионный договор №980КС/12-2023 / 3010-06/01-24 от 24.01.2024 с 24.01.2024 по 11. 01.2025), Электронная библиотека ВГУ, Договор №ДС-208 от 01.02.2021 с ООО «ЦКБ «БИБКОМ» и ООО «Агентство «Книга-Сервис» о создании Электронной библиотеки ВГУ, (с 01.02.2021 по 31.01.2027), ЭБС BOOK.ru, Договор №3010 15/983 23 от 20.12.2023, (с 01.02.2024 по 31.01.2025)

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)

№ п/п	Источник
1	Пирогов В.Ю. Ассемблер и дизассемблирование / В.Ю. Пирогов. – СПб.: БХВ-Петербург, 2006. - 464 с.
2	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors : Обнаружение и защита / О.В. Зайцев. – СПб. : БХВ-Петербург, 2006. - 304 с.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Для реализации учебного процесса используется установленная версия пакета среды виртуализации Oracle VM VirtualBox; образы операционных систем семейства Windows v.7, 8, 10; тестовые дистрибутивы антивирусных программ и средств анализа уязвимостей; доступ в сеть Интернет; LibreOffice v.5-7; Foxit PDF Reader; Справочно-правовая система (СПС) Консультант+ для образования.

При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения

Moodle, развернутой в университете, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

1) Учебная аудитория (компьютерный класс) (одна из №1-4 корп. 1а, ауд. № 382-385): специализированная мебель, персональные компьютеры на базе i5-9600KF-3,7ГГц, мониторы ЖК 24'' (16 шт.), специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

2) Для проведения лабораторных работ. Компьютерный класс (один из №1-3 корп. 1а, ауд. № 290, 293, 383), ПК-Intel-i7 16 шт. (с оперативной памятью не менее 8 гигабайт, рекомендуется 16 гигабайт), специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Разделы 1-6, 8. Основные технологии разработки и внедрения вредоносных программ. Основные направления защиты от вредоносных программ	ПК-1	ПК-1.3	Устный опрос. Лабораторные работы 1-8. Контрольная работа по соответствующим разделам или тест
2.	Разделы 6-8 Основные направления защиты от вредоносных программ	ПК-3	ПК-3.1	Устный опрос. Лабораторные работы 6-8. Контрольная работа по соответствующим раз-делам или тест
3.	Разделы 1-8 Требования по обеспечению антивирусной защиты в государственных информационных системах и информационных системах персональных данных Основные направления защиты от вредоносных программ		ПК-3.2	Устный опрос. Лабораторные работы 1-8. Контрольная работа по соответствующим разделам или тест
Промежуточная аттестация форма контроля – контрольная работа				Комплект КИМ

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета.

Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных

средств:

Устный опрос; Контрольная работа по теоретической части курса; Лабораторные работы

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 20.2
3	Лабораторная работа	Содержит 15 лабораторных заданий, предусматривающие разработку требований по уровням и классам защищенности различных информационных систем, разработки и внедрения их систем защиты, а также контроля ее эффективности.	При успешно выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену, в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену.
4	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 вопроса для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 20.2

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине

Компетенция ПК-1

Задания закрытого типа

1. **На каких этапах жизненного цикла государственной информационной системы должна обеспечиваться в ней защита информации от вредоносных программ?**

а) на этапе создания информационной системы;

б) на этапе создания информационной системы и в ходе ее эксплуатации;

в) на этапе создания информационной системы, в ходе ее эксплуатации, в том числе при развитии (модернизации);

г) должна носить систематический характер и осуществляться как на этапе создания системы, так и в ходе ее эксплуатации, в том числе при развитии (модернизации);

д) на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации;

2. **На каких этапах жизненного цикла государственной информационной системы должна осуществляться оценка угроз внедрения и использования вредоносных программ?**

а) на этапе создания информационных систем;

б) на этапе создания информационных систем и в ходе их эксплуатации;

в) на этапе создания информационных систем, в ходе их эксплуатации, в том числе при развитии (модернизации);

г) должна носить систематический характер и осуществляться как на этапе создания систем, так и в ходе их эксплуатации, в том числе при развитии (модернизации).

д) на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации;

3. **Чем удостоверяется соответствие антивирусного средств защиты информации, требованиям по защите информации?**

а) аттестатом соответствия;

б) лицензией;

в) сертификатом соответствия;

г) аттестатом аккредитации;

4. Меры по антивирусной защите должны обеспечивать:

а) обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;

в) обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия;

г) регистрацию событий безопасности, сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них;

д) обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации;

5. Формирование требований к защите информации, содержащейся в государственной информационной системе, предполагает следующие этапы:

а) принятие решения о необходимости защиты информации; классификацию информационной системы по требованиям защиты информации; определение угроз безопасности информации; определение требований к системе защиты информации;

б) анализ рисков нарушения информационной безопасности; разработку модели угроз безопасности информации; определение требований к системе защиты информации;

в) анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система; определение угроз безопасности информации; определение требований к системе защиты информации;

г) определение информации, подлежащей защите в информационной системе и ее значимости; классификации информационной системы по требованиям защиты информации; определение угроз безопасности информации; определение требований к системе защиты информации;

6. В качестве исходных данных для определения угроз безопасности информации, содержащейся в государственной информационной системе, используется:

а) банк данных угроз безопасности информации (bdu.fstec.ru), а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации;

б) модель угроз безопасности информации, а также результаты анализа уязвимостей информационной системы;

в) модель угроз безопасности информации, результаты анализа уязвимостей информационной системы, а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации;

г) банк данных угроз безопасности информации (bdu.fstec.ru), а также результаты анализа уязвимостей информационной системы;

7. Реализация антивирусной защиты в государственной информационной системе и/или в информационной системе персональных данных должна предусматривать:

а) применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы);

б) установку, конфигурирование и управление средствами антивирусной защиты;

в) предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;

г) проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);

д) проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;

е) оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);

ж) определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами);

з) все вышеперечисленное;

Задания открытого типа

1. Возможна ли разработка универсальной антивирусной или вредоносной программы?
2. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации если они повлекли тяжкие последствия или создали угрозу их наступления наказываются лишением свободы на срок до
3. Какие основные требования антивирусной защиты информации в государственных информационных системах?
4. Какие основные требования антивирусной защиты информации в информационных системах персональных данных?
5. Какие основные требования антивирусной защиты информации в информационных системах общего пользования 1-го класса?

Задания с развёрнутым ответом

1. **Какие основные мероприятия антивирусной защиты информации проводятся в государственной информационной системе?**

Критерии оценивания	Шкала оценок
Обучающийся приводит основные мероприятия антивирусной защиты информации в государственных информационных системах. Подробно описан каждый из этапов.	Отлично (90-100 баллов)
Обучающийся приводит основные мероприятия антивирусной защиты информации в государственных информационных системах. Подробно описан каждый из этапов. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Обучающийся допускает ошибку в последовательности основных мероприятий антивирусной защиты информации в государственных информационных системах. Частично описан каждый из этапов. Ответ не содержит грубых ошибок.	Удовлетворительно (50-70 баллов)
Не представлены этапы антивирусной защиты информации в государственных информационных системах. Присутствуют грубые ошибки или неточности.	Неудовлетворительно

Компетенция ПК-3

Задания закрытого типа

1. **Правила и процедуры антивирусной защиты информационной системы регламентируются в**

а) руководстве администратора;
б) руководстве пользователя;
в) эксплуатационной документации;
г) организационно-распорядительных документах;

2. Реализация и управление антивирусной защитой в государственных информационных системах требуется для

а) 1 класса защищенности;
б) 1 и 2 классов защищенности;
в) 1, 2 и 3 классов защищенности;

3. Реализация и управление антивирусной защитой в государственных информационных системах в виртуальной инфраструктуре требуется для

а) 1 класса защищенности;
б) 1 и 2 классов защищенности;
в) 1, 2 и 3 классов защищенности;

4. Реализация и управление антивирусной защитой в информационных системах персональных данных требуется для

а) 1 уровня защищенности;
б) 1 и 2 уровней защищенности;
в) 1, 2 и 3 уровней защищенности;
г) 1, 2, 3 и 4 уровней защищенности;

5. Реализация и управление антивирусной защитой в информационных системах персональных данных в виртуальной инфраструктуре требуется для

а) 1 уровня защищенности;
б) 1 и 2 уровней защищенности;
в) 1, 2 и 3 уровней защищенности;
г) 1, 2, 3 и 4 уровней защищенности;

6. В каких информационных системах в целях защиты информации предусмотрено обязательное применение сертифицированных средств антивирусной защиты информации?

а) в государственных информационных системах;
б) в информационных системах персональных данных;
в) в информационных системах общего пользования;
г) во всех вышеперечисленных информационных системах;

7. В каких информационных системах в целях защиты информации предусмотрено обязательное применение антивирусных средств, сертифицированных ФСБ России?

а) в государственных информационных системах;
б) в информационных системах персональных данных;
в) в информационных системах общего пользования 1-го класса;
г) во всех перечисленных выше информационных системах;

Задания открытого типа

1. Какие основные требования антивирусной защиты информации в государственных информационных системах?
2. Какие основные требования антивирусной защиты информации в информационных системах персональных данных?
3. Какие основные требования антивирусной защиты информации в информационных системах общего пользования 1-го класса?
4. Возможно ли внедрение вредоносной программы при просмотре веб-страницы в информационно-телекоммуникационной сети Интернет?
5. Возможно ли внедрение вредоносной программы при просмотре электронного документа?
6. Для обеспечения защиты информации, содержащейся в государственной информационной системе, применяются антивирусные средства защиты информации, прошедшие оценку соответствия в форме обязательной

Задания с развёрнутым ответом

1. **Как проводится анализ уязвимостей информационной системы на этапе ее эксплуатации и оценка возможностей реализации угрозы внедрения вредоносного кода?**

Критерии оценивания	Шкала оценок
Обучающийся приводит основные приемы и средства анализа уязвимостей информационной системы. Подробно описаны основные возможности.	Отлично (90-100 баллов)
Обучающийся приводит основные приемы и средства анализа уязвимостей информационной системы. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Обучающийся допускает ошибку в описании приемов и средств анализа уязвимостей информационной системы. Ответ не содержит грубых ошибок.	Удовлетворительно (50-70 баллов)
Не представлены основные приемы и средства анализа уязвимостей информационной системы. Присутствуют грубые ошибки или неточности.	Неудовлетворительно

20.2. Промежуточная аттестация

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

При оценивании могут использоваться количественные или качественные шкалы оценок.

Для оценивания результатов обучения при проведении промежуточной аттестации используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание нормативных документов, основных определений, понятий и используемой терминологии;

2) умение проводить обоснование требований нормативных документов и практических мер их реализующих с использованием с использованием сертифицированных средств защиты информации;

3) умение связывать требования нормативных документов с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторно-практических заданий;

4) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

5) владение навыками программирования и администрирования компьютерных систем и средств защиты в рамках выполняемых лабораторных заданий;

6) владение навыками проведения компьютерного эксперимента, тестирования компьютерных моделей алгоритмов обработки информации.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено,

не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на зачете

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

20.3. Примерный перечень практических заданий, тем рефератов, тем презентаций, докладов, вопросов к зачету с оценкой

№	Содержание
1	Классификация вредоносных программ
2	Признаки присутствия на компьютере вредоносных программ
3	Модель компьютерного вируса
4	Модель сетевого червя
5	Оценка потенциальных алгоритмических свойств вредоносных программ
6	Возможности использования программы обнаружения вредоносных программ AVZ
7	Отладчики и дизассемблеры. Основные возможности отладчика IDA.
8	Классификация антивирусных программ и их основные возможности
9	Основные возможности и способы компьютерной разведки
10	Возможности сетевых сканеров обнаружения уязвимостей (на примере СканерВС).
11	Основные средства и их возможности защиты компьютерной сети
12	Возможности низкоуровневого воздействия вредоносных программ. Программы-шпионы (кейлогеры)
13	Модель угроз безопасности информации. Современные тенденции развития вредоносных программ
14	Программа APS (Anti Port Scanner) и её возможности
15	Современные методики оценки уязвимостей информационных систем
16	Основные возможности антивирусной программы Kaspersky Internet Security
17	Основные возможности антивирусной программы и особенности применения Kaspersky Endpoint Security

20.4. Пример задания для выполнения лабораторной работы

Лабораторная работа № 2

«Исследование возможностей наиболее распространенных антивирусных программ. Особенности использования программы обнаружения вредоносных программ AVZ. Скрипты и управление AVZ»

Цель работы:

Исследовать возможности антивирусных средств защиты информации.

Форма контроля: отчёт в электронном виде

Количество отведённых аудиторных часов: 4

Задание:

Получите у преподавателя вариант задания, образ операционной системы и дистрибутив антивирусного средства. Для ответа на поставленные вопросы требуется проинсталлировать антивирусное средство на виртуальную машину. Оценить возможности антивирусного средства. Разработайте скрипт управления антивирусным средством в соответствии с вариантом задания. Составьте отчёт о проделанной работе, в котором отразите следующие пункты:

- ФИО исполнителя и номер группы.
- Название и цель лабораторной работы.
- Номер своего варианта.
- Код, написанный исполнителем.
- Краткие выводы об исследованных возможностях антивирусного средства.

Примеры контрольных вопросов:

1. Какие основные параметры операционной системы может контролировать AVZ.
2. Какие возможности контроля предоставляют скрипты управления антивирусным средством.

Варианты заданий:

1. Разработка скрипта для сканирования сети.
2. Лечение заданных папок по заданному условию.
3. Сканирование и помещение подозрительных файлов на автокарантин.
4. Обновление баз с протоколированием
5. Разработка скрипта удаления троянской программы с известным именем.
6. Разработка скрипта сканирования и отправки результатов по почте.
7 Разработка скрипта контроля целостности заданных файлов.

20.5. Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2021

Направление подготовки / специальность 10.03.01 Информационная безопасность

Дисциплина Б1.В.04 Защита от вредоносных программ

Форма обучения Очное

Вид контроля зачет с оценкой

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Классификация вредоносных программ.

2. Основные возможности и особенности применения антивирусной программы Kaspersky Endpoint Security.

Преподаватель _____ С.А. Вялых