Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Сирота Александр Анатольевич

Кафедра технологий обработки и защиты информации

23.04.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.44 Защита программ и данных

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

Разработка защищенного программного обеспечения

3. Квалификация (степень) выпускника:

Специалист

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Дрюченко Михаил Анатольевич, к.т.н., доцент

7. Рекомендована:

протокол №5 от 05.03.2024

8. Учебный год:

2027-2028

9. Цели и задачи учебной дисциплины:

Цель дисциплины – ознакомление студентов с теоретическими и практическими аспектами защиты программ и данных от широкого класса угроз информационной безопасности.

Основные задачи дисциплины: ознакомление студентов с основными угрозами информационной безопасности, концепциями и аспектами обеспечения информационной безопасности, типовыми программно-аппаратными средствами и системами защиты информации, методами и средствами анализа уязвимостей и защиты программ, принципами создания защищенного ПО, методами и средствами защиты данных от угроз нарушения конфиденциальности, целостности и доступности, современными технологиями и инструментами обеспечения безопасности информации в компьютерных сетях.

10. Место учебной дисциплины в структуре ООП:

базовый блок дисциплины в обще-профессиональной части. Для успешного освоения дисциплины

необходимы входные знания в области основ информационной безопасности, сетей и систем передачи информации, операционных систем, языков программирования, криптографии, цифровой обработки сигналов, навыки программирования.

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

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.14	знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Знает основные виды технической разведки, возможности современных технических средств перехвата информации, методы организации, способы и средства защиты информации от утечки по техническим каналам.
		ОПК-5.15	знает организацию защиты информации от утечки по техническим каналам на объектах информатизации	
		ОПК-5.16	знает возможности технических средств перехвата информации	
ОПК-7	Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ОПК-7.5	умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач	Знает технологии программирования, методологии и технологии проектирования, разработки, отладки и тестирования ПО на языках высокого уровня. Умеет применять на практике полученные знания и навыки для разработки, отладки и тестирования ПО при решении типовых профессиональных задач. Владеет практическими навыками проектирования, разработки, отладки, тестирования и документирования ПО.
		ОПК-7.6	владеет навыками разработки, документирования, тестирования и отладки программ	
		ОПК-7.9	знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения	
		ОПК-7.10	умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач	

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ОПК-13	Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности	ОПК-13.18	Умеет применять средства и методы анализа программного обеспечения для выявления закладок	Знает основные методы анализа ПО на наличие закладок и уязвимостей, методы статического и динамического анализа программ, методы проведения экспертизы исходного кода, программные методы защиты и предотвращения несанкционированного доступа к данным. Умеет применять на практике известные средства и методы анализа ПО для проверки его работоспособности, выявления закладок и обнаружения уязвимостей, современные средства обеспечения информационной безопасности программ и данных. Умеет проводить анализ программных средств, применяемых для контроля и защиты информации, аттестацию программ и алгоритмов на предмет соответствия требованиям защиты информации. Владеет специализированными инструментами и практическими навыками анализа ПО на наличие закладок и уязвимостей, навыками анализа программных средств и алгоритмов на предмет соответствия требованиям защиты информации
		ОПК-13.19	Умеет применять методы анализа проектных решений для обеспечения защищенности компьютерных систем	
		ОПК-13.20	Знает программные методы предотвращения несанкционированного доступа к данным	
		ОПК-13.21	Уметь применять современные средства обеспечения информационной безопасности программ и данных	
		ОПК-13.22	Знает основные программные методы защиты данных от несанкционированного доступа	
		ОПК-13.23	Умеет проводить анализ программных средств, применяемых для контроля и защиты информации	
		ОПК-13.24	Умеет проводить аттестацию программ и алгоритмов на предмет соответствия требованиям защиты информации	
ОПК-16	Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	ОПК-16.11	Знает основные виды деструктивных воздействий на программные продукты	Знает виды деструктивных воздействий на программные продукты, современные методы анализа программных решений по обеспечению защищенности компьютерных систем. Умеет применять на практике специализированные инструменты для выявления действий вредоносных программ и определения характера их воздействия. Владеет практическими навыками защиты от компьютерных вирусов и других вредоносных программам, методами и средствами защиты информации.
		ОПК-16.12	Умеет выявлять действие вредоносных программ, и определять характер их воздействия	
		ОПК-16.13	Знает современные методы анализа программных решений по обеспечению защищенности компьютерных систем	

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Экзамен

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 8	Всего
Аудиторные занятия	42	42
Лекционные занятия	28	28
Практические занятия	0	0
Лабораторные занятия	14	14
Самостоятельная работа	30	30
Курсовая работа		0
Промежуточная аттестация	0	0
Часы на контроль	36	36
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн- курса, ЭУМК
		1. Лекции	
1.1	Методы и средства защиты данных от несанкционированного доступа. Криптографические методы защиты данных	Классификация технических каналов утечки информации. Виды технических разведок. Модель канала утечки информации. Способы и средства защиты данных от утечки по техническим каналам. Противодействие несанкционированного доступа к данным в компьютерных системах. Защита конфиденциальности, контроль целостности и аутентичности программ и данных с использованием базовых криптографических преобразований.	Создан онлайн электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ
1.2	Методы анализ программ. Защита программ от изучения	Статический и динамический анализ программ. Принципы функционирования отладчиков и дизассемблеров. Анализ потоков данных. Методы поиска функций защиты в машинном коде. Методы анализа параллельных программ. Принципы создания безопасного ПО. Методы встраивания защиты в ПО. Методы защиты программ от отладки и дизассемблирования. Механизмы защиты от наблюдения, установки, сравнения характеристик среды, ответной реакции. Методы обфускации исходных и байт-кодов программ. Методы установки подлинности кода (tamper-proofing).	Создан онлайн электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн- курса, ЭУМК
1.3	Методы внедрения программных закладок. Противодействие программным закладкам. Защита программ и данных от вредоносного ПО и компьютерных вирусов	Классы программных закладок. Модели «наблюдатель», «перехват», «искажение». Методы внедрения программных закладок. Методы камуфлирования. Методы выявления программных закладок (сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных потоков). Классы вредоносных программ. Принцип действия и деструктивные возможности. Файловые, загрузочные, сетевые, макровирусы, троянские программы. Руткиты. Принципы работы антивирусных программ и профилактика заражения вирусами компьютерных систем.	Создан онлайн электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ
1.4	Защита программ и данных от несанкционированного копирования и распространения	Юридические, экономические и технические меры. Авторское право и патентная защита. Использование методов цифровой стеганографии для защиты авторских прав. Защита ПО и данных с использованием технологий цифровых водяных знаков (digital/software watermarking) и отпечатков пальцев (fingerprinting).	Создан онлайн электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ
1.5	Защита баз данных	Комплексный подход при защите БД. Штатный аудит и мониторинг, резервное копирование, шифрование, применение автоматизированных системы защиты (Database Activity Monitoring, Database Firewall), двухфакторная аутентификация.	Создан онлайн электронный курс, размещены материалы к лекции.
2. Лабораторные работы			
2.1	Методы и средства защиты данных от несанкционированного доступа. Криптографические методы защиты данных	1. Практическое изучение базовых криптографических методов для защиты конфиденциальности, контроля целостности и аутентичности данных.	Размещены индивидуальные задания для выполнения лабораторных работ
2.2	Методы анализ программ. Защита программ от изучения	2. Практическое изучение средств и методов защиты программ от анализа. 3. Защита ПО, основанная на идентификации пользователя, идентификации компьютера, идентификации исполняемого модуля. 4. Работа со средствами для обфускации программ.	Размещены индивидуальные задания для выполнения лабораторных работ

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн- курса, ЭУМК
2.3	Методы внедрения программных закладок. Противодействие программным закладкам. Защита программ и данных от вредоносного ПО и компьютерных вирусов	5. Практическое изучение типовых уязвимостей ПО (переполнения буфера, уязвимость форматной строки, переполнение целых) и реализация программных закладок. 6. Организация антивирусной защиты.	Размещены индивидуальные задания для выполнения лабораторных работ
2.4	Защита программ и данных от несанкционированного копирования и распространения	7. Практическое изучение механизмов внедрения водяных знаков и отпечатков пальцев в ПО и файлы различных форматов.	Размещены индивидуальные задания для выполнения лабораторных работ

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Методы и средства защиты данных от несанкционированного доступа. Криптографические методы защиты данных	6		2	6	14
2	Методы анализ программ. Защита программ от изучения	6		6	6	18
3	Методы внедрения программных закладок. Противодействие программным закладкам. Защита программ и данных от вредоносного ПО и компьютерных вирусов	6		4	6	16
4	Защита программ и данных от несанкционированного копирования и распространения	6		2	6	14
5	Защита баз данных	4			6	10
		28	0	14	30	72

14. Методические указания для обучающихся по освоению дисциплины

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 практических работ обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

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

№ п/п	Источник
1	Рябко, Борис Яковлевич. Криптография и стеганография в информационных технологиях / Б.Я. Рябко, А.Н. Фионов, Ю.И. Шокин ; Рос. акад. наук, Сиб. отд-ние, Ин-т вычисл. технологий СО РАН .— Новосибирск : Наука, 2015 .— 239 с. : ил. — Библиогр.: с.232-236 .— ISBN 978-5-02-019206-5.
2	Рябко, Борис Яковлевич. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов .— 2-е изд. — Москва : Горячая линия - Телеком, 2013 .— 232 с. : ил., табл. — Библиогр.: с.225-229.
3	Корниенко, А.А. Криптографические методы защиты информации : учебное пособие / А.А. Корниенко, М.Л. Глухарев. – Санкт-Петербург : ПГУПС, [б. г.]. – Часть 1 – 2017. – 64 с. – ISBN 978-5-7641-1053-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/111765 (дата обращения: 07.07.2023). – Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
1	Круглов И.А. Введение в теоретико-числовые методы криптографии / И.А. Круглов [и др.]. – СПб: Лань, 2011. – 400 с.
2	Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351 .— ISBN 978-5-8041-0378-2.
3	Пугин, В. В. Криптографические протоколы : учебное пособие / В. В. Пугин. – Самара : ПГУТИ, 2019. – 68 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/223319 (дата обращения: 07.07.2023). – Режим доступа: для авториз. пользователей.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
2	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
3	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)
4	ЭБС «Университетская библиотека online» (Контракт №3010 06/11 23 от 26.12.2023 (с 26.12.2023 по 25.12.2024)
5	ЭБС «Консультант студента» – Лицензионный договор №980КС/12-2023 / 3010-06/01-24 от 24.01.2024 с 24.01.2024 по 11. 01.2025)
6	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)
7	БС BOOK.ru, Договор №3010 15/983 23 от 20.12.2023, (с 01.02.2024 по 31.01.2025)

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала, работа с учебно-методической литературой, подготовка отчетов по лабораторным работам.
Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован электронный курс, на котором размещены материалы к лекции и задания к лабораторным работам.

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

Для реализации учебного процесса используются:
ПО ОС Windows v.7, 8, 10, ОС GNU/Linux (Ubuntu).
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.

18. Материально-техническое обеспечение дисциплины:

1) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 479
Учебная аудитория: специализированная мебель, компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19’’, мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

2) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 292
Учебная аудитория: специализированная мебель, компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam Group и ноутбук 15.6’’ FHD Lenovo V155-15API
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

3) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 380
Учебная аудитория: специализированная мебель, компьютер преподавателя i3-3240-3,4ГГц, монитор с ЖК 17'', мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Разделы 1,3-5 Методы и средства защиты данных от несанкционированного доступа. Криптографические методы защиты данных. Методы внедрения программных закладок. Противодействие программным закладкам. Защита программ и данных от вредоносного ПО и компьютерных вирусов Защита программ и данных от несанкционированного копирования и распространения Защита баз данных	ОПК-5	ОПК-5.14, ОПК-5.15, ОПК-5.16	Контрольная работа по разделам дисциплины. Лабораторные работы 1,5,6. Тест по соответствующим разделам
	Разделы 1-5 Методы и средства защиты данных от несанкционированного доступа. Криптографические методы защиты данных. Методы анализ программ. Защита программ от изучения. Методы внедрения программных закладок. Противодействие программным закладкам. Защита программ и данных от вредоносного ПО и компьютерных вирусов Защита программ и данных от несанкционированного копирования и распространения Защита баз данных	ОПК-7	ОПК-7.5, ОПК-7.6, ОПК-7.9, ОПК-7.10	Контрольная работа по разделам дисциплины. Лабораторные работы 1-7. Тест по соответствующим разделам
	Разделы 1-3 Методы и средства защиты данных от несанкционированного доступа. Криптографические методы защиты данных. Методы анализ программ. Защита программ от изучения Методы внедрения программных закладок. Противодействие программным закладкам. Защита программ и данных от вредоносного ПО и компьютерных вирусов	ОПК-13, ОПК-16	ОПК-13.18, ОПК-13.19, ОПК-13.20, ОПК-13.21, ОПК-13.22, ОПК-13.23, ОПК-13.24, ОПК-16.11, ОПК-16.12, ОПК-16.13	Контрольная работа по разделам дисциплины. Лабораторные работы 1-6. Тест по соответствующим разделам

Промежуточная аттестация
Форма контроля – Экзамен
Оценочные средства для промежуточной аттестации
Перечень вопросов, практическое задание

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Устный опрос на практических занятиях
Контрольная работа по теоретической части курса
Лабораторные работы

Примерный перечень применяемых оценочных средств

№ 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	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует таблице, приведенной ниже
3	Лабораторная работа	Содержит 6 заданий	При успешном 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 заданий вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкала оценивания приведена ниже

20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение семестра), проверку выполнения установленного перечня лабораторных заданий, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

Для оценки теоретических знаний используется перечень контрольно-измерительных материалов. Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает два задания - вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции. При оценивании используется количественная шкала. Критерии оценивания приведены в таблице, приведенной ниже.

Для оценивания результатов обучения на экзамене используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1. знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;
2. умение проводить обоснование и представление основных теоретических и практических результатов;
3. умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторных заданий;
4. умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;
5. владение навыками программирования в рамках выполняемых лабораторных заданий.

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 экзамене

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. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	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. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	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. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки. Не выполнены лабораторные работы в соответствии с установленным перечнем.	–	Неудовлетворительно

Примерный перечень вопросов к экзамену

№	Содержание
1	Виды технических каналов утечки информации
2	Способы и средства защиты данных от утечки по техническим каналам
3	Криптографические методы для защиты конфиденциальности данных
4	Криптографические методы для контроля целостности и аутентичности данных
5	Статический и динамический анализ программ
6	Принципы функционирования отладчиков и дизассемблеров
7	Методы поиска функций защиты в машинном коде
8	Общие принципы создания безопасного ПО
9	Методы встраивания защиты в ПО
10	Методы защиты программ от отладки и дизассемблирования
11	Методы обфускации программ
12	Методы защиты программ, основанные на идентификации пользователя
13	Методы защиты программ, основанные на идентификации компьютера
14	Методы защиты программ, основанные на идентификации исполняемого модуля
15	Программные закладки. Классы. Принципы действия
16	Методы внедрения программных закладок
17	Методы маскировки программных закладок
18	Методы выявления программных закладок
19	Вредоносное ПО. Классы. Принципы действия и деструктивные возможности
20	Руткиты
21	Принципы работы антивирусных программ. Рекомендации по профилактике заражения вирусами компьютерных систем
22	Юридические, экономические и технические меры защиты программ и данных от несанкционированного копирования и распространения
23	Использование методов стеганографии для защиты авторских прав, контроля несанкционированного копирования и распространения данных
24	Защита ПО с использованием технологий software watermarking и fingerprinting
25	Комплексный подход при защите БД
26	Принципы работы автоматизированных систем защиты БД

Пример контрольно-измерительного материала

УТВЕРЖДАЮ

Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота

__.__.2024

Направление подготовки / специальность 10.05.01 Компьютерная безопасность

Дисциплина Б1.О.44 Защита программ и данных

Форма обучения Очное

Вид контроля Экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Методы выявления программных закладок
2. Криптографические методы для контроля целостности и аутентичности данных

Преподаватель_____ М.А. Дрюченко